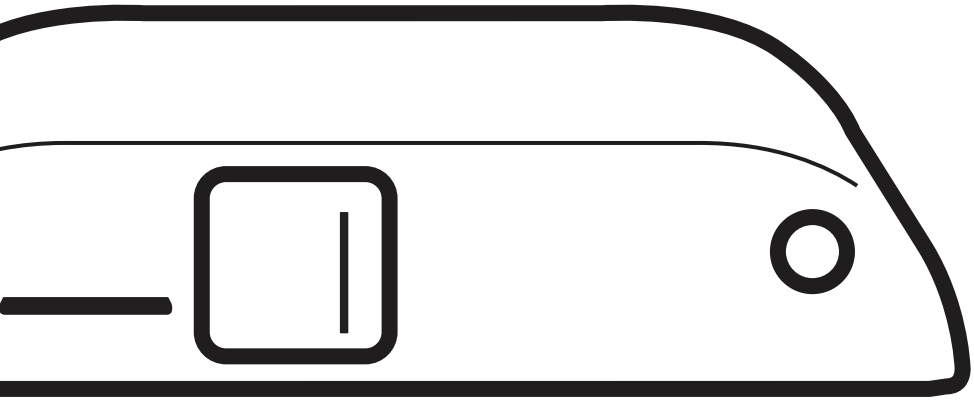
cradlepoint

Global Leader in 4G LTE Network Solutions

COR Series Router

IBR600 / IBR650

User Manual



cradlepoint.com

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

TABLE OF CONTENTS

INTRODUCTION 4

WHAT'S IN THE BOX 4

KEY FEATURES 4
WAN 4
LAN 4
MANAGEMENT 4
VPN AND ROUTING 4
SECURITY 5

SPECIFICATIONS 5

ACCESSORIES 6

BUSINESS-GRADE MODEM SPECIFICATIONS 6

HARDWARE 9

SUPPORT AND WARRANTY 9

LEDS 10

QUICK START 11

BASIC SETUP 11

ACCESSING THE ADMINISTRATION PAGES 12

FIRST TIME SETUP WIZARD 12

USING NETCLOUD MANAGER 12

ADMINISTRATION PAGES 13

QUICK LINKS 13

DASHBOARD 13

CONNECTION MANAGER 14
WAN INTERFACE PROFILES & PRIORITY 14

STATUS 18
INTERNET 18
CLIENT LIST 23
TUNNELS 23
FIREWALL 24
ROUTING 24
ETHERNET 25

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

GPS 25
SYSTEM LOGS 25

NETWORKING 26
LOCAL NETWORKS 26
VLAN INTERFACES 36
TUNNELS 37
ROUTING 49
QOS 59
DNS SERVERS 62
WIFI AS WAN 64
WAN AFFINITY 65
CLIENT DATA USAGE 67
NHRP 68

SECURITY 70
IDENTITIES 70
ZONE FIREWALL 70
CONTENT FILTERING 75
CERTIFICATE MANAGEMENT 78

SYSTEM 81
ADMINISTRATION 81
NETCLOUD 86
DEVICE ALERTS 86
SERIAL REDIRECTOR 88
GPIO CONNECTOR 88
SNMP CONFIGURATION 89
SYSTEM CONTROL 90
DIAGNOSTICS 92
SETUP WIZARDS 93

APPENDIX 96

ROUTER COMMUNICATION/DATA USAGE 96

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

INTRODUCTION

WHAT'S IN THE BOX

- COR IBR600/IBR650 Integrated Broadband Router w/ metal mounting bracket
- External 3G/4G mobile broadband modem antennas (2) (SMA) w/ support for GPS on auxiliary connection (some models), finger tighten only
- External WiFi antennas (2) reverse SMA*, 5 dBi gain, finger tighten only
- 12V / 1.5A power supply w/ locking connector; GPIO/power cable available
- Quick Start Guide with warranty information

KEY FEATURES

WAN

- LTE-only, HSPA+, or LTE/HSPA+/EVDO
- Advanced Modem Failure Check
- Standby

LAN

- VLAN 802.1Q
- DHCP Server, Client, Relay
- DNS and DNS Proxy
- DynDNS
- UPnP
- DMZ
- Multicast/Multicast Proxy
- QoS (DSCP and Priority Queuing)
- MAC Address Filtering

MANAGEMENT

- Cradlepoint NetCloud Manager[1]
- Web UI, API, CLI
- Data Usage Alerts (router and per client)
- Advanced Troubleshooting (support)
- Device Alerts
- SNMP
- SMS control

VPN AND ROUTING

- IPsec Tunnel – up to five concurrent sessions
- GRE Tunnel
- Route Filters (Access Control Lists, Prefix Filters, Route Maps, Communities for BGP)
- Routing Rules
- Policy-based Routing
- NAT-less Routing
- Virtual Server/Port Forwarding
- IPv6

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- CP Secure VPN compatible*

*-Cradlepoint Secure VPN-NAT configuration only

SECURITY

- RADIUS and TACACS+ support*
- 802.1x authentication for Ethernet
- Certificate support
- ALGs
- MAC Address Filtering
- Advanced Security Mode (local user management only)
- Per-Client Web Filtering
- IP Filtering
- Content Filtering (basic)
- Website Filtering
- Zone-Based Object Firewall with host address (IP or FQDN), port, and mac address

*-Native support for authentication. Authorization and accounting support through hotspot/captive portal services.

1 – NetCloud Manager requires a subscription

SPECIFICATIONS

WAN:

- Integrated LTE-only, HSPA+, or LTE/HSPA+/EVDO modem
- Two 10/100 Ethernet ports (WAN or LAN)

LAN: Two 10/100 Ethernet ports (WAN or LAN)

PORTS:

- Power
- Two Ethernet LAN or WAN
- Two cellular antenna connectors (SMA)
- Two WiFi connectors* (reverse SMA)

TEMPERATURE:

- -20 °C to 60 °C (-4 °F to 140 °F) operating modem as WAN
- -20 °C to 50 °C (-4 °F to 122 °F) operating Ethernet as WAN
- -30 °C to 70 °C (-22 °F to 158 °F) storage

HUMIDITY (non-condensing):

- 10% to 85% operating
- 5% to 90% storage

POWER:

- DC input steady state voltage range: 9 – 18VDC
- Recommended inline fuse for vehicle installations: 1.5A fast-blow
- **IDLE:**
  - typical=350mA@12V(4.2W)

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

  - worst case=700mA@12V(8.4W)
- **TX/RX:**
  - typical=600mA@12V(7.2W)
  - worst case=1200mA@12V(14.4W)

SIZE: 3.3 x 4.0 x 0.9 in (85 x 102 x 22 mm)

CERTIFICATIONS:
- FCC
- WiFi Alliance*
- Shock/Vibration (MIL STD 810G and SAEJ1455)
- Carrier certifications (see individual SKUs for additional certifications)

*-IBR600 only

ACCESSORIES

- Universal 3G/4G/LTE antenna w/ SMA connector (2dBi/3dBi) (Part # 170649-000)
- Directional Patch antenna for external (outside) mounting (Part # 170587-000)
- Directional Yagi (Log-Periodic) antenna for external (outside) mounting (Part # 170588-000)
- Omni-directional antenna for external (outside) mounting (Part # 170586-000)
- 12" Mag-mount antenna (Part # 170605-000)
- 4" Mini mag-mount antenna (Part # 170606-000)
- COR 2 meter power & GPIO cable (direct wire) (Part # 170585-000)
- COR 2 meter power & GPIO cable (direct wire) with filter (required for E-mark compliant vehicle installations) (Part # 170635-100)
- COR vehicle power adapter (Part # 170635-000)
- COR wall power adapter (Part # 170584-000)
- COR international wall power adapter (Part # 170446-002)
- COR mounting bracket (Part # 170593-000)

See the Cradlepoint antenna accessories page for more information about antennas. Also see the Antenna Ordering and Installation Guide, available as a PDF in the Resources section of antenna and router product pages.

BUSINESS-GRADE MODEM SPECIFICATIONS

COR IBR600/IBR650 models include an integrated 4G LTE or HSPA+ or LTE/HSPA+/EVDO modem – specific model names include a specific modem (e.g., the COR IBR650LPE-VZ includes a Verizon LTE modem).

COR IBR600LPE-VZ, COR IBR650LPE-VZ – 4G LTE/HSPA+/EVDO for Verizon
- **Technology:** LTE, HSPA+, EVDO Rev A
- **Downlink Rates:** LTE 50 Mbps, HSPA+ 21.1 Mbps, EVDO 3.1 Mbps (theoretical)
- **Uplink Rates:** LTE 50 Mbps, HSPA+ 5.76 Mbps, EVDO 1.8 Mbps (theoretical)
- **Frequency Bands:**
  - LTE: Band 2 (1900 MHz), Band 4 – AWS (1700/2100 MHz), Band 5 (850 MHz), Band 13 (700 MHz), Band 17 (700 MHz), Band 25 (1900 MHz)

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

  - HSPA+/UMTS: (850/900/1900/2100 MHz, AWS)
  - GSM/GPRS/EDGE: (850/900/1800/1900 MHz)
  - CDMA EVDO: Rev A/1xRTT (800/1900 MHz)
- **Power:** LTE 23 dBm +/- 1, HSPA+ 23 dBm +/- 1, EVDO 24 dBm +/- 1 (typical conducted)
- **Antennas:** two SMA male (plug), finger tighten only (maximum torque spec is 7 kgfcm)
- **Industry Standards & Certs:** FCC, WiFi Alliance (IBR600 only), Verizon, Verizon NEMO/DMNR for Primary Wireless Access
- **SIM:** one 2FF slot
- **GPS:** passive GPS support

COR IBR600LPE-AT, COR IBR650LPE-AT – 4G LTE/HSPA+/EVDO for AT&T

- **Technology:** LTE, HSPA+, EVDO Rev A
- **Downlink Rates:** LTE 50 Mbps, HSPA+ 21.1 Mbps, EVDO 3.1 Mbps (theoretical)
- **Uplink Rates:** LTE 50 Mbps, HSPA+ 5.76 Mbps, EVDO 1.8 Mbps (theoretical)
- **Frequency Bands:**
  - LTE: Band 2 (1900 MHz), Band 4 – AWS (1700/2100 MHz), Band 5 (850 MHz), Band 13 (700 MHz), Band 17 (700 MHz), Band 25 (1900 MHz)
  - HSPA+/UMTS: (850/900/1900/2100 MHz, AWS)
  - GSM/GPRS/EDGE: (850/900/1800/1900 MHz)
  - CDMA EVDO: Rev A/1xRTT (800/1900 MHz)
- **Power:** LTE 23 dBm +/- 1, HSPA+ 23 dBm +/- 1, EVDO 24 dBm +/- 1 (typical conducted)
- **Antennas:** two SMA male (plug), finger tighten only (maximum torque spec is 7 kgfcm)
- **Industry Standards & Certs:** PTCRB, FCC, WiFi Alliance (IBR600 only), AT&T
- **SIM:** one 2FF slot
- **GPS:** passive GPS support

COR IBR600LPE-SP, COR IBR650LPE-SP – 4G LTE/HSPA+/EVDO for Sprint

- **Technology:** LTE, HSPA+, EVDO Rev A
- **Downlink Rates:** LTE 50 Mbps, HSPA+ 21.1 Mbps, EVDO 3.1 Mbps (theoretical)
- **Uplink Rates:** LTE 50 Mbps, HSPA+ 5.76 Mbps, EVDO 1.8 Mbps (theoretical)
- **Frequency Bands:**
  - LTE: Band 2 (1900 MHz), Band 4 – AWS (1700/2100 MHz), Band 5 (850 MHz), Band 13 (700 MHz), Band 17 (700 MHz), Band 25 (1900 MHz)
  - HSPA+/UMTS: (850/900/1900/2100 MHz, AWS)
  - GSM/GPRS/EDGE: (850/900/1800/1900 MHz)
  - CDMA EVDO: Rev A/1xRTT (800/1900 MHz)
- **Power:** LTE 23 dBm +/- 1, HSPA+ 23 dBm +/- 1, EVDO 24 dBm +/- 1 (typical conducted)
- **Antennas:** two SMA male (plug), finger tighten only (maximum torque spec is 7 kgfcm)
- **Industry Standards & Certs:** FCC, WiFi Alliance (IBR600 only), Sprint
- **SIM:** one 2FF slot
- **GPS:** passive GPS support

COR IBR600LPE-GN, COR IBR650LPE-GN – 4G LTE/HSPA+/EVDO (generic – for use on T-Mobile and US Cellular in the U.S. and Rogers, Bell, & TELUS in Canada)

- **Technology:** LTE, HSPA+, EVDO Rev A
- **Downlink Rates:** LTE 50 Mbps, HSPA+ 21.1 Mbps, EVDO 3.1 Mbps (theoretical)
- **Uplink Rates:** LTE 50 Mbps, HSPA+ 5.76 Mbps, EVDO 1.8 Mbps (theoretical)
- **Frequency Bands:**
  - LTE: Band 2 (1900 MHz), Band 4 (AWS), Band 5 (850 MHz), Band 13 (700 MHz), Band 17 (700 MHz), Band 25

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

(1900 MHz)
    - HSPA+/UMTS: (850/900/1900/2100 MHz, AWS)
    - GSM/GPRS/EDGE: (850/900/1800/1900 MHz)
    - CDMA EVDO: Rev A/1xRTT (800/1900 MHz)
- **Power:** LTE 23 dBm +/– 1, HSPA+ 23 dBm +/– 1, EVDO 24 dBm +/– 1 (typical conducted)
- **Antennas:** two SMA male (plug), finger tighten only (maximum torque spec is 7 kgfcm)
- **Industry Standards & Certs:** CE, WiFi Alliance (IBR600 only), GCF-CC
- **SIM:** one 2FF slot
- **GPS:** passive GPS support

COR IBR600LP3-EU, COR IBR650LP3-EU
- **Technology:** LTE, HSPA+
- **Downlink Rates:** LTE 50 Mbps, HSPA+ 21 Mbps (theoretical)
- **Uplink Rates:** LTE 50 Mbps, HSPA+ 5.76 Mbps (theoretical)
- **Frequency Bands:**
    - LTE Band 1 (2100 MHz), Band 3 (1800 MHz), Band 7 (2600 MHz), Band 8 (900 MHz), Band 20 (800 MHz)
    - HSPA+/UMTS: (800/850/900/1900/2100 MHz)
    - GSM/GPRS/EDGE: (850/900/1800/1900 MHz)
- **Module Power:** LTE 23 dBm +/- 1, UMTS 23dBm +/- 1 (typical conducted)
- **Module Antennas:** two SMA male (plug), 2 dBi gain; finger tighten only; maximum torque spec is 7 kgf-cm
- **Industry Standards & Certs:** CE, WiFi Alliance (IBR600 only), GCF-CC
- **SIM:** one 2FF slot
- **GPS:** passive GPS support

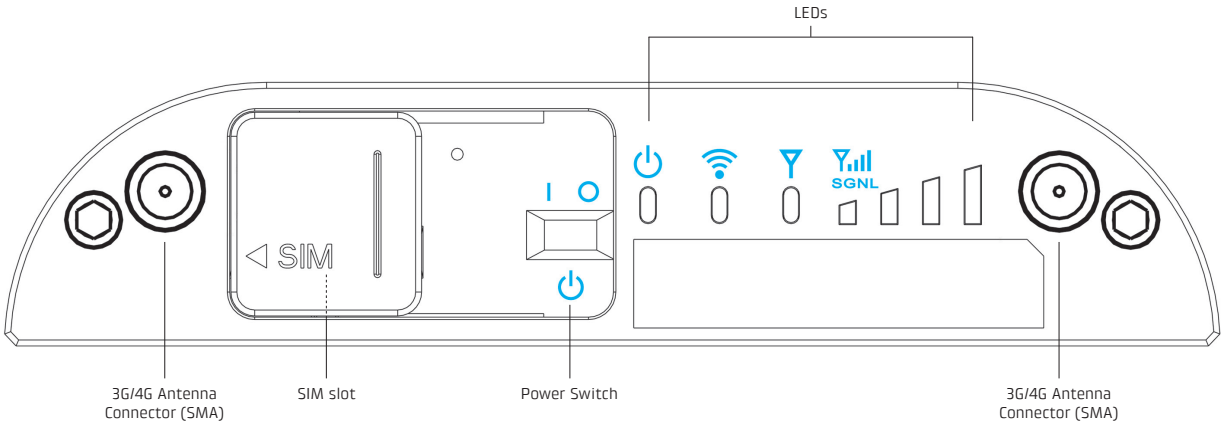
COR IBR600P-INTL, COR IBR650P-INTL
- **Technology:** HSPA+
- **Downlink Rates:** HSPA+ 21 Mbps (theoretical)
- **Uplink Rates:** HSPA+ 5.76 Mbps (theoretical)
- **Frequency Bands:**
    - HSPA+/UMTS: (800/850/900/1900/2100 MHz)
    - GSM/GPRS/EDGE: (850/900/1800/1900 MHz)
- **Module Power:** LTE 23 dBm +/- 1, UMTS 23dBm +/- 1 (typical conducted)
- **Module Antennas:** two SMA male (plug), 2 dBi gain; finger tighten only; maximum torque spec is 7 kgf-cm
- **Industry Standards & Certs:** PTCRB, GCF-CC, FCC, IC, CE, WiFi Alliance (IBR600 only)
- **SIM:** one 2FF slot
- **GPS:** passive GPS support

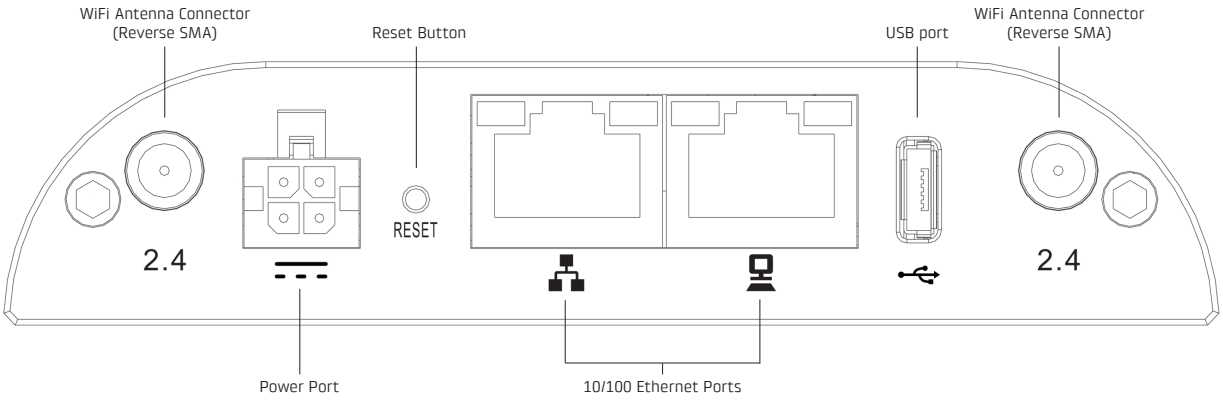
Cradlepoint products with the -EU and -INTL SKUs enable and disable WiFi channels to comply with EU law. The -EU and -INTL SKUs are not legal for use in North America.

The -EU and -INTL versions come with an adapter kit for non-USA/Canada power outlets (includes US, EU, and UK options).

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

HARDWARE





SUPPORT AND WARRANTY

CradleCare Support available in the US and Canada with technical support, software upgrades, and advanced hardware exchange – 1-, 3-, and 5-year options.

Three-year limited hardware warranty available world-wide on IBR600/IBR650 series products when purchased from an approved Cradlepoint Partner or Distributor – extend warranty to 5 years.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

LEDS

INDICATOR	BEHAVIOR
	POWER The Cradlepoint IBR600/IBR650 must be powered using an approved 12 V DC power source. • Blue = Powered ON. • No Light = Not receiving power. Check the power switch and the power source connection.
	WiFi BROADCAST Indicates WiFi activity (IBR600 only). • Green = WiFi is on and operating normally. • Amber = Attention. Open the administration pages and check the router status.
	INTEGRATED OR USB MODEM Indicates information about the integrated modem or attached USB modem. • Green = Modem has established an active connection. • Blinking Green = Modem is connecting. • Amber = Modem is not active. • Blinking Amber = Data connection error. No modem connection possible. • Blinking Red = Modem is in the process of resetting.
	SIGNAL STRENGTH Blue LED bars indicate the active modem's signal strength. • 4 Solid Bars = Strongest signal. • 1 Blinking Bar = Weakest signal. (A blinking bar indicates half of a bar.)
Other	**ADDITIONAL LED INDICATIONS** • Several different LEDs blink when the factory reset button is detected. • Two of the modem LEDs blink red in unison for 10 seconds when there is an error during NCOS upgrade.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

QUICK START

BASIC SETUP

1. Insert an activated SIM

A wireless broadband data plan must be added to your Cradlepoint IBR600/IBR650. Wireless broadband data plans are available from wireless carriers such as Verizon, AT&T, Sprint, EE, and Vodafone. The SIM must be provisioned with the carrier. Contact your carrier for details about selecting a data plan and about the process for provisioning your SIM.

Insert the card with the notch-end first and the gold contacts facing down – it will click into place.

2. Attach the WiFi and modem antennas

Attach the two WiFi antennas and two modem antennas to the connectors. Antennas are jointed, which enables you to position them for optimal signal. To attach, hold the antenna straight and twist the base of the antenna to connect, folding the joint if needed. *NOTE: Ensure that the router antennas are not near metal or other RF reflective surfaces.*

3. Connect the power source

Plug the provided power supply into an electrical outlet. Then connect the power supply to the router.

4. Ensure power is switched on

O = OFF
– = ON

5. Connect to a computer or other network equipment

For the IBR650, simply connect your device(s) to the router via Ethernet.

1. On a WiFi-enabled computer or device, open the window or dropdown menu that allows you to access wireless networks. The IBR600 network will appear on the list: select this network.
2. Log in. You will need to input the **Default Password** when prompted. The **Default Password** is provided on the product label found on the bottom of your router (this password is the last eight digits of the router's MAC address, which can be found on the product box or on the product label).

cradlepoint
Part:IBR600LPE-VZ
Default Password: 4414f6aa
IMEI: 356 1950 5005 2891
MEID: 35 6195 0500 5289
WiFi MAC ID: 0030 4414 f6aa
Serial No.: MM14030123456
SSID: IBR600-6aa
WiFi CERTIFIED
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions (1) This device may not cause harmful interference and (2)This device must accept any interference received, including interference that may cause undesired operation
FC ID:UXX-IBR600E
IC:6921A-IBR600E
Contains FCC ID: N7NMC7355
Contains IC:2417C-MC7355
Model:IBR600LPE
Made in Taiwan 12V 1.5A H/W:1.3 www.cradlepoint.com
1288-405
E467298

NOTE: If more than one IBR600 wireless router is visible, you can find the correct unit by checking for its SSID (service set identifier; the unique name of the local network). The default SSID of the primary network has the form IBR600-xxx, where "xxx" is the last 3 digits of the router's MAC address.

NOTE: The product label above is an example only: your **DEFAULT PASSWORD** *and* **SSID** *will be unique.*

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

ACCESSING THE ADMINISTRATION PAGES

Once you are connected, open the Cradlepoint IBR600's GUI-based administration pages to make configuration changes to your router.

1. Open a browser window and type "**cp/**" or "**192.168.0.1**" in the address bar. Press **ENTER/RETURN**.
2. When prompted for your password, type the eight character **DEFAULT PASSWORD** found on the product label.

It's possible – and more efficient – to do all your configuration changes through Cradlepoint **NetCloud Manager** (NCM) without logging into the local administration pages. Set up a group of routers and set the configuration for all of them at once. See **below** for more information about NCM.

FIRST TIME SETUP WIZARD

When you log in for the first time, you will be automatically directed to the **FIRST TIME SETUP WIZARD**, which will walk you through the steps to customize your Cradlepoint IBR600/IBR650. You have the ability to configure any of the following:

- Administrator Password
- Time Zone
- WiFi Network Name
- Security Mode
- Access Point Name (APN) for SIM-based modems
- Modem Authentication
- Failure Check

If you are currently using the router's WiFi network, you will need to reconnect your devices to the network using the newly established wireless network name and password.
NOTE: To return to the First Time Setup Wizard after your initial login, select **SYSTEM** *from the navigation bar, expand* **Setup Wizard**, *and select* **First Time Setup**.

USING NETCLOUD MANAGER

Rapidly deploy and dynamically manage networks at geographically distributed stores and branch locations with **NetCloud Manager**, Cradlepoint's next generation management and application platform. NetCloud Manager (NCM) integrates cloud management with your Cradlepoint devices to improve productivity, increase reliability, reduce costs, and enhance the intelligence of your network and business operations.

Click **here** to sign up for a free 30-day NCM trial.

Depending on your ordering process, your devices may have already been bulk-loaded into NCM. If so, simply log in at **cradlepointecm.com** using your NCM credentials and begin managing your devices seamlessly from the cloud.

If your device has not yet been loaded into your NCM account, you need to register. Log into the device administration pages and select **NetCloud** from the **SYSTEM** menu. Enter your NCM username and password, and click on "Register".

Once you have registered your device, go to **cradlepointecm.com** and log in using your NCM credentials.

For more information about how to use Cradlepoint NetCloud Manager, see the following:

- **Getting Started**
- **NCM on the Knowledge Base**

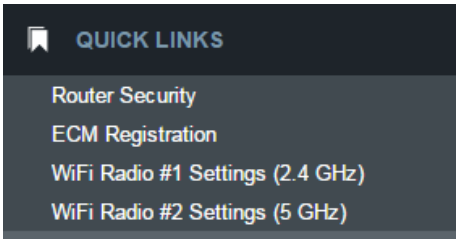
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

ADMINISTRATION PAGES

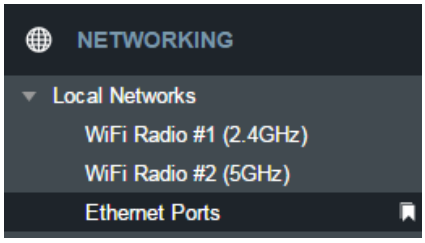
Quick Links
Dashboard
Connection Manager
Status
Networking
Security
System

QUICK LINKS

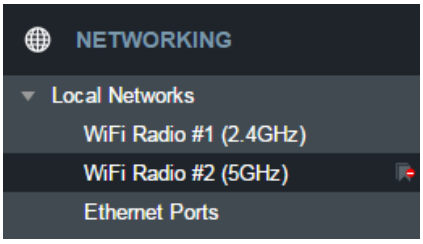
Quick Links allows you to bookmark your most commonly-used settings. Simply click on the bookmark icon ( ) to add an item to your Quick Links menu. To remove an item from your Quick Links menu, select the item and click on the remove bookmark icon ( ).



Quick Links Menu

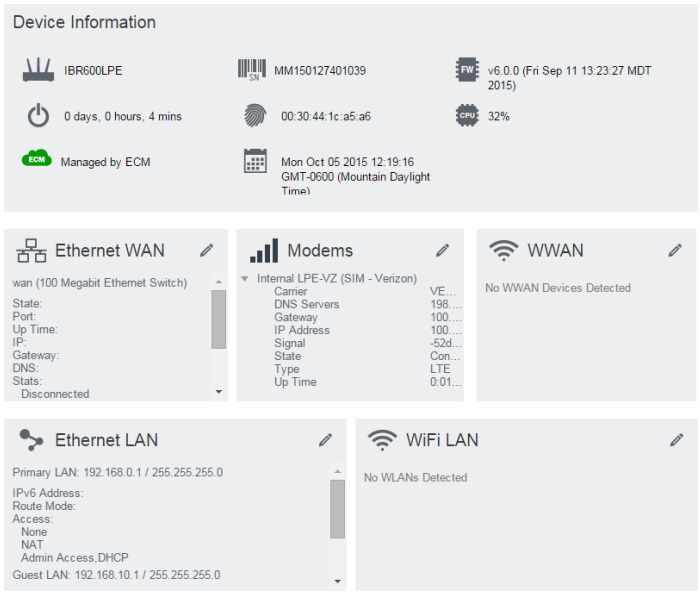


Add Quick Link



Delete Quick Link

DASHBOARD



The **Dashboard** is a centralized location for basic information about the status of your router. The areas include:

- Device Information
- Ethernet WAN*
- Modems*
- WWAN*
- Ethernet LAN*
- WiFi LAN*

*-To quickly edit settings for any of these areas, click on the pencil icon ( ) in the top-right of the desired dialog box.

You may return to the Dashboard at any time by clicking on **DASHBOARD** from the left menu or by clicking on the Cradlepoint logo at the top-left of the screen.

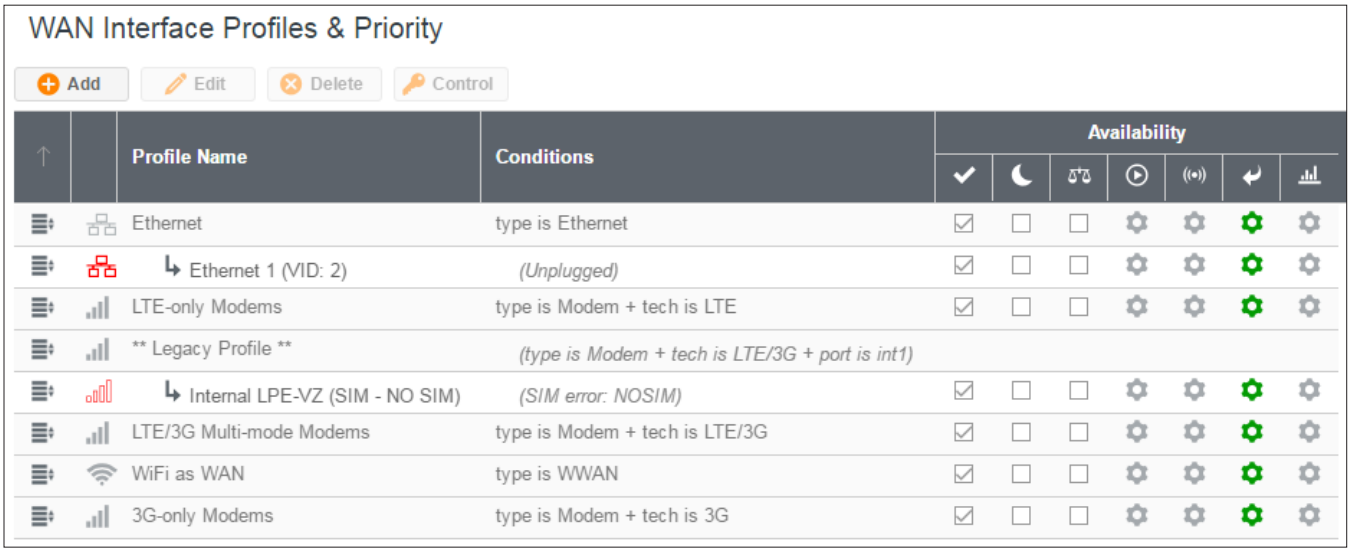
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

CONNECTION MANAGER

The router can establish an uplink via Ethernet, WiFi as WAN, or 3G/4G modems (removable or external USB). If the primary WAN connection fails, the router will automatically attempt to bring up a new link on another device: this feature is called **failover**. If Load Balance is enabled, multiple WAN devices may establish a link concurrently.

WAN INTERFACE PROFILES & PRIORITY

This is a list of the available interfaces used to access the Internet. You can enable, stop, or start devices from this section. Drag the priority icon (≡) up or down to set the interface the router uses by default and the order that it allows failover.



Availability Key

- Enable
- Standby
- Load Balance
- On Demand
- WAN Verify
- Failback
- Data Usage

STANDBY

Standby is used to decrease failover time from one WAN interface to another. When Standby is enabled for a WAN profile or interface, the relevant interfaces are kept in a connected-but-idle (minimal, non-routed traffic) state. When the current WAN connection is disrupted, the traffic will failover to the next priority WAN. If that interface is on Standby, the connection is already established and failover will take much less time.

Note that the current connected interface(s) is/are indicated by a green connection state. For interfaces on Standby, the interface is indicated by a yellow connection state. If the interface is indicated in red, the interface is not currently connected or in Standby.

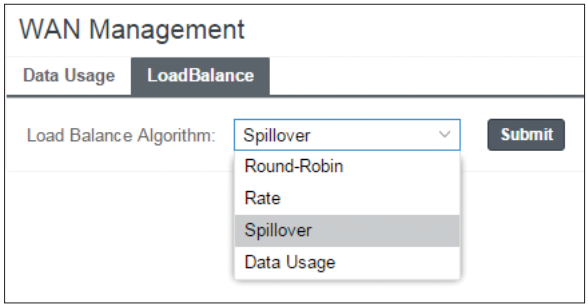
Standby is used to enable faster failover times only. If you want to manage traffic to a specific WAN interface, you will need to use WAN Affinity. If WAN Affinity is enabled for a particular profile or interface, do not enable Standby for that profile or interface as the failover results may vary and be unexpected.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

LOAD BALANCE

To enable Load Balancing, select the check box for each desired device. If this is enabled, the router will use multiple WAN interfaces to increase the data transfer throughput by using any connected WAN interface consecutively. Selecting Load Balance will automatically start the WAN interface and add it to the pool of WAN interfaces to use for data transfer. Turning off Load Balance for an active WAN interface may require the user to restart any current browsing session.

From **WAN Management**, select the **Load Balance Algorithm** from the following dropdown options:

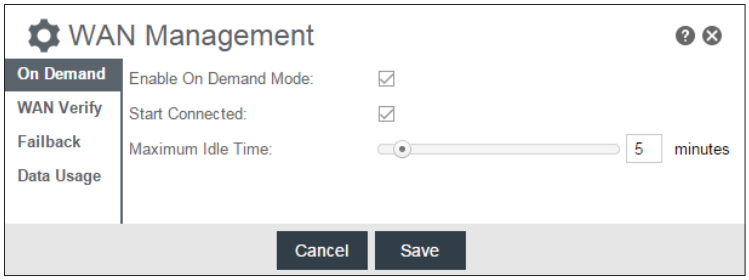


- **Round-Robin**: Evenly distribute each session to the available WAN connections.
- **Rate**: Distribute load based on the current upload and download rates. A WAN device's upload and download bandwidth values can be set in **Internet > Connection Manager**.
- **Spillover**: This was the default algorithm in older (version 3) firmware. Load is always given to devices with the most available bandwidth. The estimated bandwidth rate is based on a combination of the upload and download configuration values and the observed capabilities of the device.
- **Data Usage**: This mode works in concert with the Data Usage feature (**Internet > Data Usage**).

The router will make a best effort to keep data usage between interfaces at a similar percentage of the assigned data cap in the data usage rule for each interface, rather than distributing sessions based solely on bandwidth. For proper functioning you need to create data usage rules for each WAN device you will be load balancing. Make certain to select the "Use with Load Balancing" checkbox in the data usage rule editor.

ON DEMAND

Typically, modem connections are not always on. When the On Demand mode is selected a connection to the Internet is made as needed. When On Demand is not selected a connection to the Internet is always maintained.



WAN VERIFY

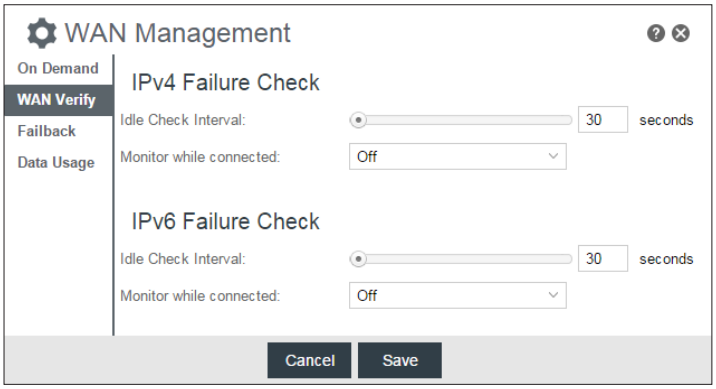
If this is enabled, the router will check that the highest priority active WAN interface can get to the Internet even if the WAN connection is not actively being used. If the interface goes down, the router will switch to the next highest priority interface available. If this is not selected, the router will still failover to the next highest priority interface but only after the user has attempted to get out to the Internet and failed.

Idle Check Interval: The amount of time between each check. (Default: 30 seconds. Range: 10-3600 seconds.)

Monitor while connected: (Default: Off) Select from the following dropdown options:

- **Passive DNS** (modem only): The router will take no action until data is detected that is destined for the WAN. When this data is detected, the data will be sent and the router will check for received data for two seconds. If no data is received the router behaves as described below under **Active DNS**.

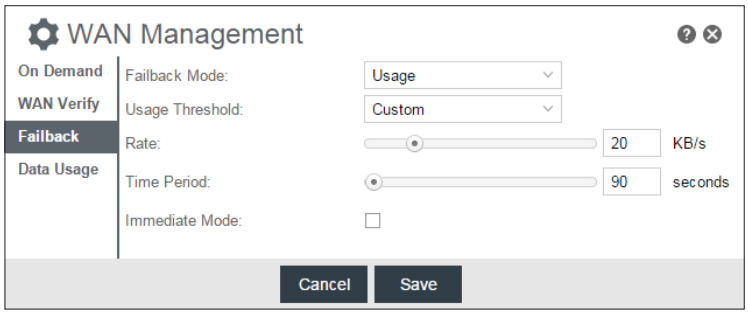
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com



- **Active DNS** (modem only): A DNS request will be sent to the DNS servers. If no data is received, the DNS request will be retried four times at five-second intervals. (The first two requests will be directed at the Primary DNS server and the second two requests will be directed at the Secondary DNS server.) If still no data is received, the device will be disconnected and failover will occur.
- **Active Ping**: A ping request will be sent to the Ping Target. If no data is received, the ping request will be retried four times at five-second intervals. If still no data is received, the device will be disconnected and failover will occur. When "Active Ping" is selected, the next line gives an estimate of data usage in this form: "Active Ping could use as much as **9.3 MB** of data per month." This amount depends on the **Idle Check Interval**.
- **Off**: Once the link is established the router takes no action to verify that it is still up.

FAILBACK

This is used to configure failback, which is the ability to go back to a higher priority WAN interface if it regains connection to its network.



Select the **Failback Mode** from the following options:

- Usage
- Time
- Disabled

Usage Threshold: Fail back based on the amount of data passed over time. This is a good setting for when you have a dual-mode EVDO/WiMAX modem and you are going in and out of WiMAX coverage. If the router has failed over to EVDO it will wait until you have low data usage before bringing down the EVDO connection to check if a WiMAX connection can be made.

- High (Rate: 80 KB/s. Time Period: 30 seconds.)
- Normal (Rate: 20 KB/s. Time Period: 90 seconds.)
- Low (Rate: 10 KB/s. Time Period: 240 seconds.)
- Custom (Rate range: 1-100 KB/s. Time Period range: 10-300 seconds.)

Time: Fail back only after a set period of time. (Default: 90 seconds. Range: 10-300 seconds.) This is a good setting if you have a primary wired WAN connection and only use a modem for failover when your wired connection goes down. This ensures that the higher priority interface has remained online for a set period of time before it becomes active (in case the connection is dropping in and out, for example).

Disabled: Deactivate failback mode.

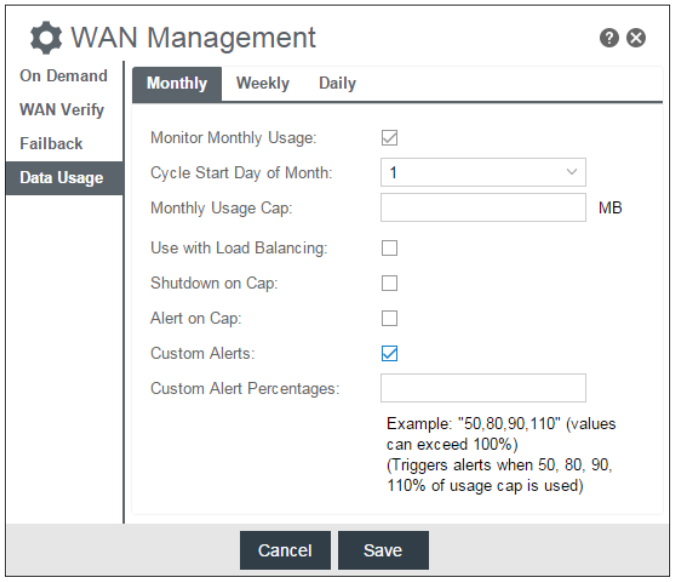
Immediate Mode: Fail back immediately whenever a higher priority interface is plugged in or when there is a priority change. Immediate failback returns you to the use of your preferred Internet source more quickly which may have advantages such as reducing the cost of a failover data plan, but it may cause more interruptions in your network than Usage or Time modes.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

DATA USAGE

Data Usage displays upload and download traffic for each LAN client. Check **Monitor Monthly** (or Weekly or Daily) **Usage** to begin tracking this information. This data is not retained between router reboots.

For **Monthly** and **Weekly** you are able to specify the day to start each cycle (e.g. the 1st or Tuesday, respectively).



Usage Cap: Enter a Cap amount in Megabytes. 1024 Megabyte is equal to 1 Gigabyte.

Use with Load Balancing: When checked, the Load Balancing feature is allowed to use the thresholds and metrics of this rule when making balance decisions. This causes Load Balancing to spread the data usage between interfaces according to the assigned usage rather than bandwidth. This is a best effort to keep all interfaces with these rules at a similar percentage utilization of data (e.g. 10%, 50%, 90%) as the cycle progresses, rather than quickly using 100% of a fast 1GB capped interface while using only a fraction of a slow 10GB capped interface, thus leaving the rest of the cycle with only the slow interface. The Data Usage algorithm on the WAN Affinity/Load Balancing page must be selected or this checkbox has no effect.

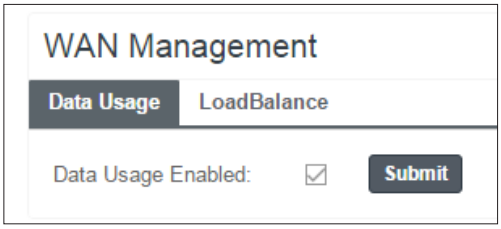
Shutdown on Cap: When checked, the WAN device will shutdown when the assigned usage is reached. A cycle reset or a rule deletion will re-enable the device.

Alert on Cap: An email alert will be generated and sent when the assigned data cap is reached. **NOTE:** The SMTP mail server must be configured in **System > Device Alerts**.

Custom Alerts: Check to enable custom alerts at specified percentage of usage cap.

Custom Alert Percentages: *Example*: "50,80,90,110" (values can exceed 100%) (Triggers alerts when 50, 80, 90, 110% of usage cap is used)

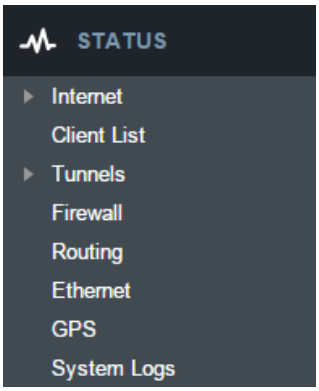
NOTE: To enable data usage, check **Data Usage Enabled** from WAN Management.



©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

STATUS

Internet
Client List
Tunnels
Firewall
Routing
Ethernet
GPS
System Logs

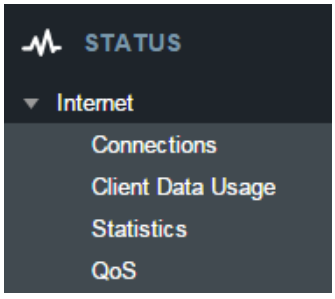


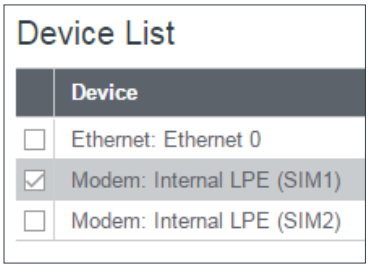
INTERNET

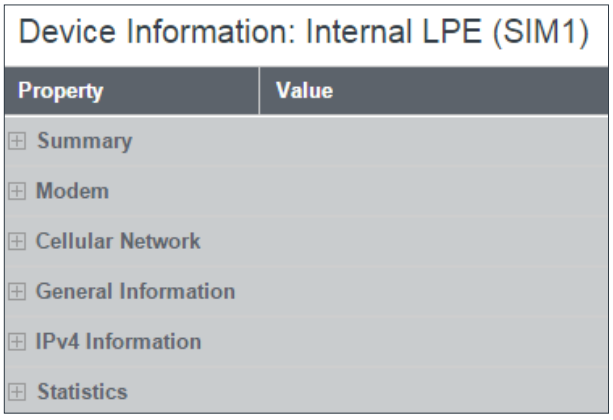
CONNECTIONS

Select your device to reveal detailed information about the following device properties:

- Summary
- Modem
- Cellular Network
- General Information
- IPv4 Information
- Statistics







©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Property	Value
Summary	
State	connected
Manufacturer	Cradlepoint Inc.
Model	Internal LPE (SIM1)
Modem Firmware Ver...	SWI9X15C_05.05.16.02 r21040 carmd-fw
Service Display	LTE
Home Carrier	Verizon
Roaming Status	Home
Signal Strength	100 %
RSSI	-53 dBm
SINR	22.2 dB
RSRP	-81 dB
RSRQ	-8 dB
Mobile Directory Num...	[redacted]
MEID	[redacted]
IMEI	[redacted]
Network Address Ide...	[redacted]
Current APN	VZWINTERNET
IP Address	100.97.122.176
Netmask	255.255.255.252
Gateway	100.97.122.177
DNS Servers	198.224.164.135,198.224.160.135

Property	Value
Summary	
Modem	
Manufacturer	Cradlepoint Inc.
Product	Internal LPE (SIM1)
Model	Internal LPE (SIM1)
Supported Technologies	lte/3g
Firmware Version	SWI9X15C_05.05.16.02 r21040 ca
Package Version	05.05.16.02_VZW,005.013_010
Mobile Directory Number	[redacted]
ESN/IMEI	[redacted]
MEID	[redacted]
IMEI	[redacted]
ICCID	[redacted]
Mobile Subscriber Identification	[redacted]
IMSI	311480206582221
PRI ID	9903437
PRI Version	05.03
PIN Status	READY
Chipset	9X15C
Hardware Version	1.0

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Property	Value
⊞ Summary	
⊞ Modem	
⊟ Cellular Network	
Home Carrier	Verizon
Roaming Status	Home
Carrier Status	UP
Connection State	Active
Service Display	LTE
Signal Strength	100 %
RSSI	-53 dBm
SINR	19.4 dB
RSRP	-80 dB
RSRQ	-12 dB
Profile 1:	vzwims
Profile 2:	vzwadmin
Profile 3:	**VZWINTERNET**
Profile 4:	vzwapp
Profile 5:	vzw800
Profile 6:	vzwadmin
Profile 9:	vzwims
Profile 10:	vzwadmin
Profile 11:	VZWINTERNET
Profile 12:	vzwapp
Profile 13:	
Cell ID	2965526 (0x2d4016)
Operating Mode	Online
System Mode	LTE
IMS Registration State	In Progress
PS State	Attached
PRL Version	15414
RF Band	Band 4
Bandwidth	10 MHz
RX Channel	2000
TX Channel	20000
LTE Tx Power	-3.0 dBm
RX Frequency Band	2110-2155 MHz
TX Frequency Band	1710-1755 MHz
EMM State	Registered
EMM Sub State	Normal Service
EMM Connection State	RRC Connected
Network Address Identifier (NAI)	[redacted]
Profile	0 Enabled
Home Address	0.0.0.0
Primary Home Agent	255.255.255.255
Secondary Home Agent	255.255.255.255
MN-AAA SPI	2
MN-HA SPI	300
MN-AAA SS	Set
MN-HA SS	Set
Reverse Tunneling	1
EVDO AAA Auth Status	Not Requested
Home PLMN ID	311480
Tracking Area Code	2817

Property	Value
⊞ Summary	
⊞ Modem	
⊞ Cellular Network	
⊟ General Information	
Unique Identifier	6ddc068b
Port	int1
Type	mdm
Model	Internal LPE (SIM1)

Property	Value
⊞ Summary	
⊞ Modem	
⊞ Cellular Network	
⊞ General Information	
⊟ IPv4 Information	
IP Address	100.67.93.1
Netmask	255.255.255.252
Gateway	100.67.93.2
DNS Servers	198.224.164.135,198.224.160.135

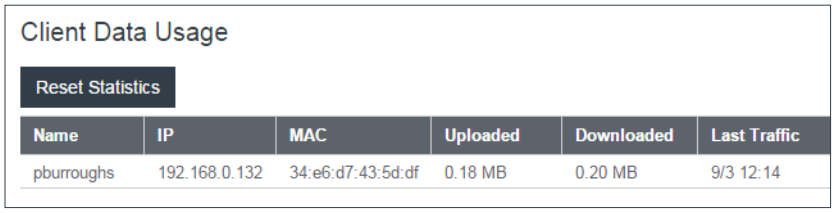
Property	Value
⊞ Summary	
⊞ Modem	
⊞ Cellular Network	
⊞ General Information	
⊞ IPv4 Information	
⊟ Statistics	
Outgoing Bytes	288098
Incoming Bytes	144940
Connection Uptime	0:08:00

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

CLIENT DATA USAGE

Displays the following client information:

- Name
- IP Address
- MAC Address
- Data Uploaded
- Data Downloaded
- Last Traffic



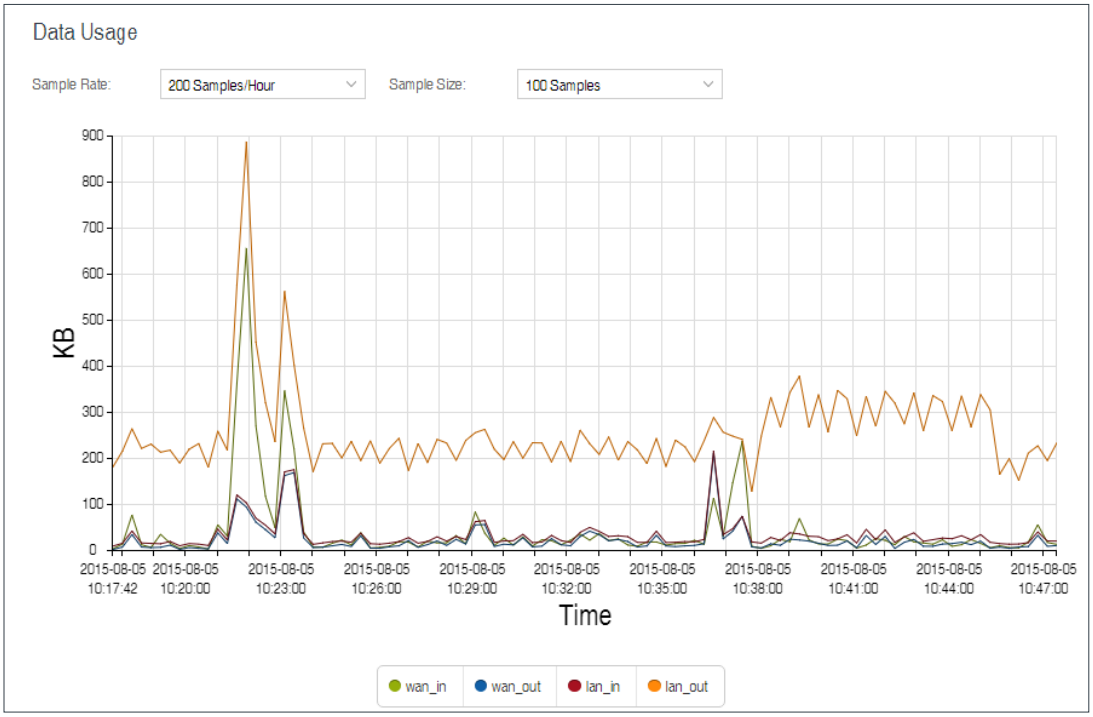
To reset information, click **Reset Statistics**.

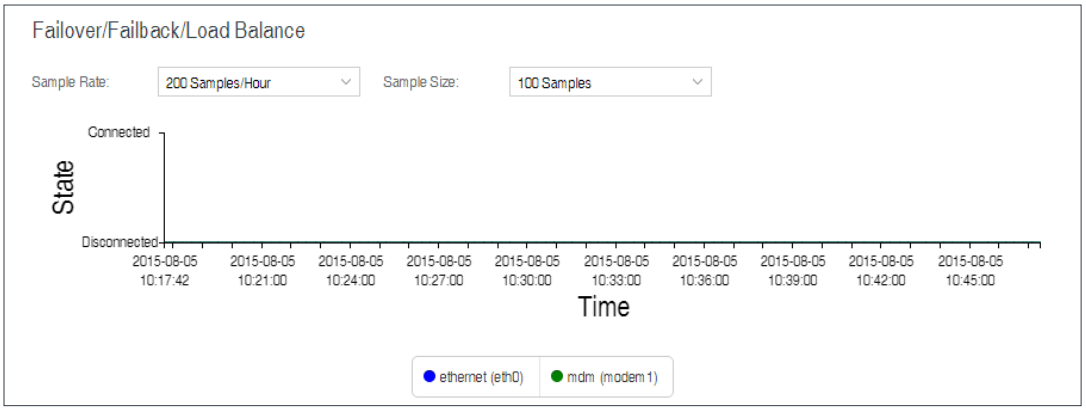
STATISTICS

Statistics can be gathered at variable Sample Rate and Sample Size for the following areas:

- Wireless Device
- Data Usage
- Failover/Failback/Load Balance

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com





QOS

Displays packets and bytes transmitted and received by your Quality of Service (QoS) queues. To enable and configure QoS, go to **NETWORKING > QoS**.

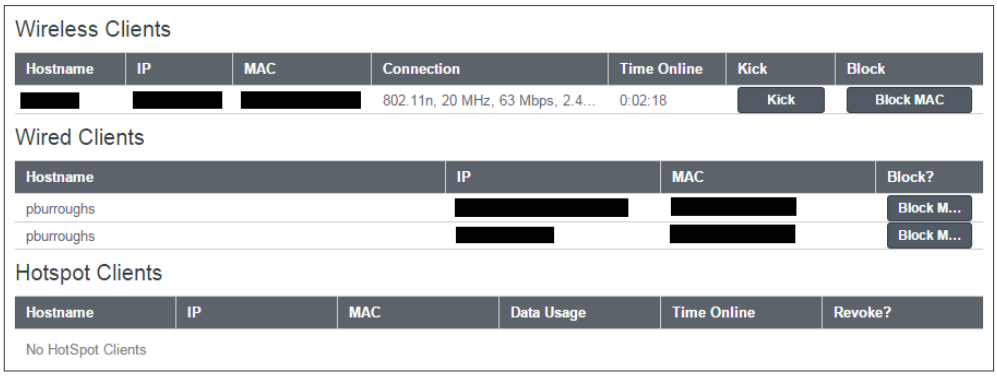
QoS

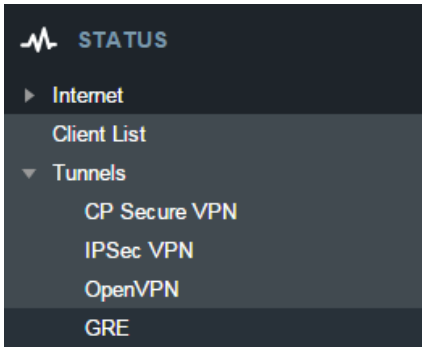
Queue	Transmit (packets/bytes)	Receive (packets/bytes)
Default	1455 / 213.70 KB	834 / 231.41 KB
test	29 / 4.30 KB	26 / 11.95 KB

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

CLIENT LIST

Displays information about your Wireless, Wired, and Hotspot Clients, and allows you to Kick Wireless Clients, block MAC addresses of both Wireless and Wired Clients, and Revoke Hotspot Clients.





TUNNELS

CP SECURE VPN

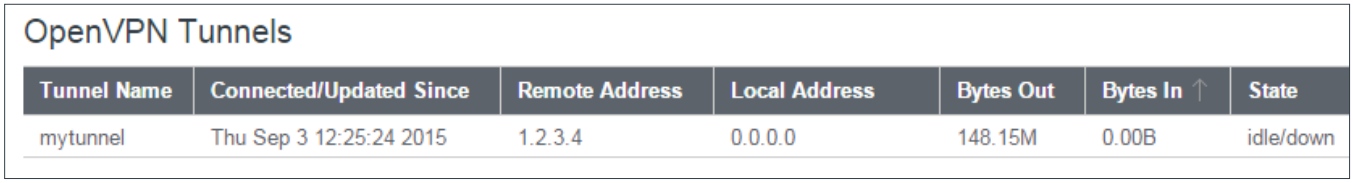
Displays status of your CP Secure VPN Tunnels. To add and configure CP Secure VPN Tunnels, go to **NETWORKING > Tunnels > CP Secure VPN**.

IPSEC VPN

Displays status of your IPSec VPN Tunnels. To add and configure IPSec VPN Tunnels, go to **NETWORKING > Tunnels > IPSec VPN**.

OPEN VPN (ONLY ON IBR600)

Displays status of your OpenVPN Tunnels. To add and configure OpenVPN Tunnels, go to **NETWORKING > Tunnels > OpenVPN**.



©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

GRE

Displays status of your GRE Tunnels. To add and configure GRE Tunnels, go to **NETWORKING > Tunnels > GRE**.

GRE Tunnels

Name	Status	Transmit (packets/bytes)	Receive (packets/bytes)	MTU
mytunnel	Tunnel Not Alive	5 / 120.00 bytes	0 / 0.00 bytes	1476

FIREWALL

Displays information about your Firewall Connection Tracking States. To configure your firewall, select **SECURITY** from the left navigation.

Connection Tracking States

Flush

Proto	Timeout	TCP State	Status	Orig Src	Orig Dst	Orig Dst Port	Reply Src	Reply Dst	Reply Dst Port
TCP	431919	ESTABL...	seen_reply,as...	100.98.9...	52.24.50.2	8001	52.24.50.2	100.98.9...	58870
TCP	64	TIME_W...	seen_reply,as...	192.168....	63.110.6...	443	63.110.6...	100.98.9...	56273
TCP	64	TIME_W...	seen_reply,as...	192.168....	63.110.6...	443	63.110.6...	100.98.9...	56272
TCP	431956	ESTABL...	seen_reply,as...	192.168....	98.138.1...	443	98.138.1...	100.98.9...	54903
TCP	431999	ESTABL...	seen_reply,as...	192.168....	192.168....	80	192.168....	192.168....	56101
TCP	62	SYN_SE...	confirmed,sna...	192.168....	172.18.4...	445	172.18.4...	100.98.9...	56317
TCP	65	TIME_W...	seen_reply,as...	192.168....	63.110.6...	443	63.110.6...	100.98.9...	56289

ROUTING

Displays information about your System, GRE, and NEMO Routes. To configure these routes, go to **NETWORKING > Tunnels**.

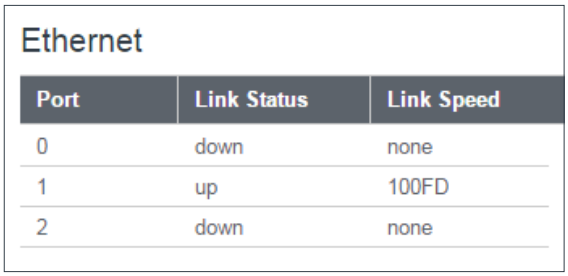
System Routes

IP Address	Gateway	Netmask	Interface	Metric	Routing Protocol
1.2.3.0		24	*iface:tun0	0	
100.107.201.144		30	9cd858ae	0	
192.168.0.0		24	primarylan	0	
192.168.10.0		24	guestlan	0	
fe80::		64	primarylan	256	

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

ETHERNET

Displays information about your Ethernet ports. To configure Ethernet ports, go to **NETWORKING > Local Networks > Ethernet Ports**.

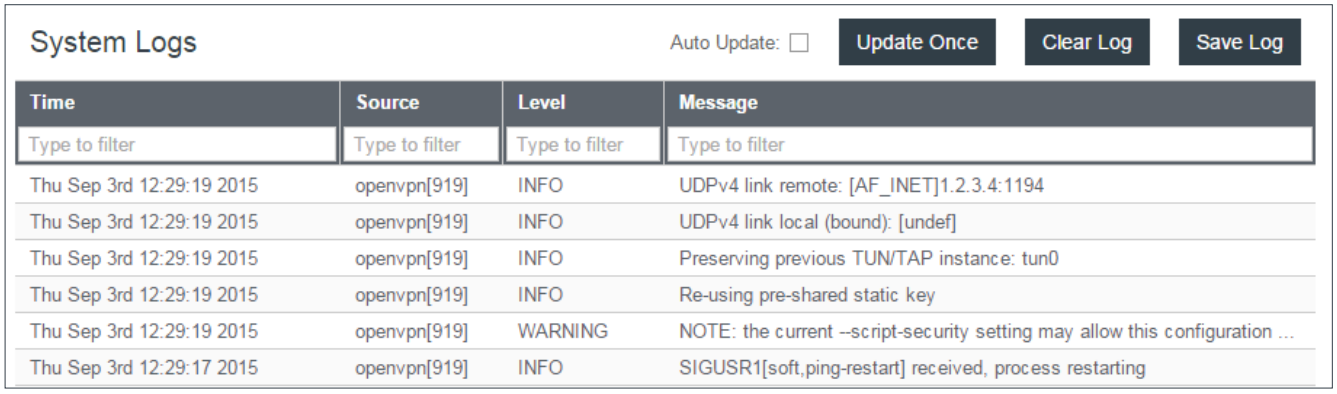


GPS

Displays GPS location and status. To enable and configure GPS, go to **SYSTEM > Administration > GPS**.

SYSTEM LOGS

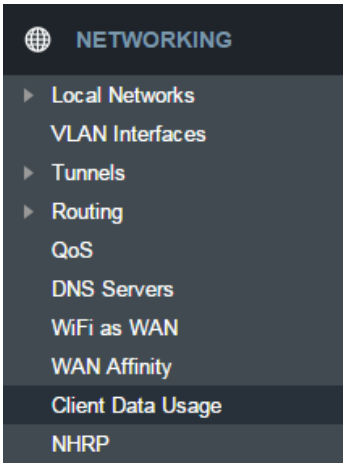
Displays System Log information. To configure System Logging, go to **SYSTEM > Administration > System Logging**.


System Logs
Auto Update:
Update Once
Clear Log
Save Log
Time
Source
Level
Message
Type to filter
Type to filter
Type to filter
Type to filter
Thu Sep 3rd 12:29:19 2015 openvpn[919] INFO UDPv4 link remote: [AF_INET]1.2.3.4:1194
Thu Sep 3rd 12:29:19 2015 openvpn[919] INFO UDPv4 link local (bound): [undef]
Thu Sep 3rd 12:29:19 2015 openvpn[919] INFO Preserving previous TUN/TAP instance: tun0
Thu Sep 3rd 12:29:19 2015 openvpn[919] INFO Re-using pre-shared static key
Thu Sep 3rd 12:29:19 2015 openvpn[919] WARNING NOTE: the current --script-security setting may allow this configuration ...
Thu Sep 3rd 12:29:17 2015 openvpn[919] INFO SIGUSR1[soft,ping-restart] received, process restarting

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

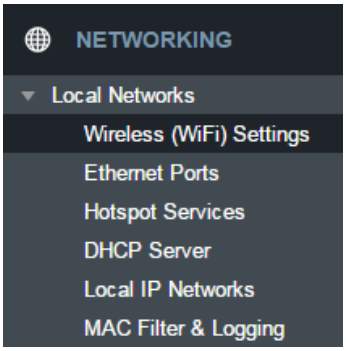
NETWORKING

Local Networks
VLAN Interfaces
Tunnels
Routing
QoS
DNS Servers
WiFi as WAN
WAN Affinity
Client Data Usage
NHRP



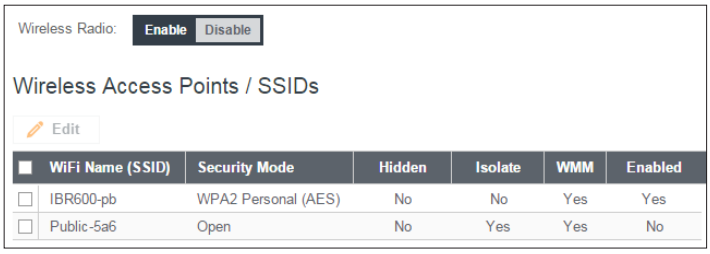
LOCAL NETWORKS

WIRELESS (WIFI) SETTINGS



WiFi Name (SSID): When users browse for available wireless networks, this is the name that they will see. This name is referred to as the SSID (service set identifier). For security purposes, Cradlepoint highly recommends that you change this from the pre-configured name.

Security Mode: You have several options for selecting a security mode. The mode you choose depends on the security features your wireless adapters support.



- WPA2 Personal
- WPA / WPA2 Personal
- WPA2 Enterprise
- WPA / WPA2 Enterprise
- WEP Auto
- Open

Select "Open" to create a hotspot: otherwise select the best security that your devices will support (Cradlepoint recommends **WPA2**).

Depending on which Security Mode you select, there are different setup options.

- "**Personal**" security modes require passwords.
- "**Enterprise**" security modes are linked to a RADIUS server and require RADIUS authentication: **IP**, **Port**, and **Shared Key** (Secondary IP and NAS ID optional).

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- "**WPA2**" (Personal or Enterprise) forces AES as the WPA Cipher.
- "**WPA/WPA2**" and "**WPA**" (Personal or Enterprise) allow AES, TKIP/AES, and TKIP.
- "**WEP Auto**" requires a WEP Key.
- "**Open**" has no password or other security measures.

NOTE: If you don't know whether you should choose Personal or Enterprise, assume Personal since you need to know RADIUS authentication for Enterprise.

In order to protect your network from hackers and unauthorized users, Cradlepoint highly recommends **WPA2/AES** for security if your attached devices can support it. WEP and WPA/TKIP are obsolete and have been replaced by WPA/AES. Using those security settings will cause the WiFi to limit to 802.11g modes.

NOTE: If you select one of the security modes and are unable to connect to the router afterwards, you can use the reset buttons to reset the router to its factory default state and try a different security mode instead.

Hidden: This shows whether the router broadcasts its SSID. It is somewhat harder for hackers to find and attack a router that is not broadcasting its SSID, which adds to the wireless security, but it is also more difficult for friendly users to attach to a WiFi network with a hidden SSID.

Isolate: Select this to isolate all wireless clients so they cannot directly communicate with each other on the wireless network.

WMM: WiFi Multimedia. This is a basic traffic shaping, or QoS (quality of service), system for the network. WMM works behind the scenes to set priorities for different types of traffic on your network. For example, video streams are given higher priority than print jobs, since video streams need consistent throughput.

Enabled: Whether the network is available.

When you select **Wireless (WiFi) Settings** from **Local Networks**, you have several additional options for configuring your wireless LANs under the **WiFi Settings** heading.

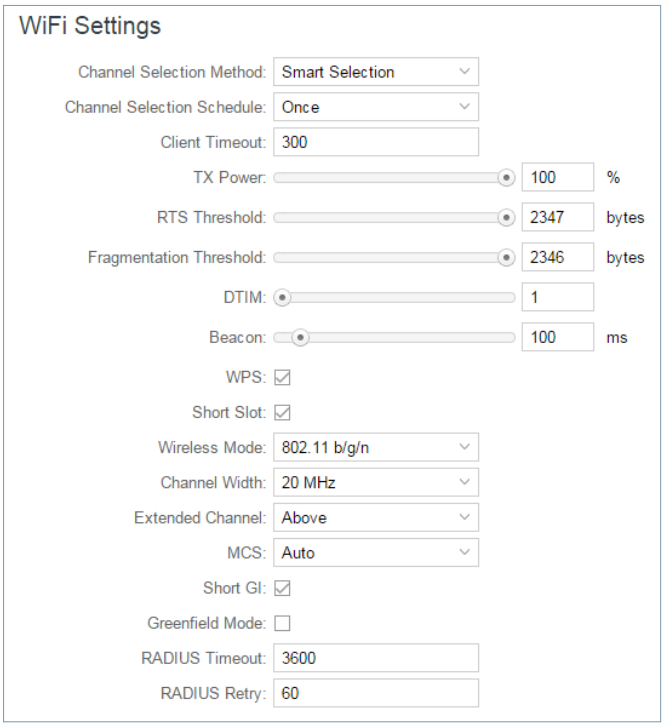
Channel Selection Method: This controls how a WiFi channel is selected.

- **User Selection** – Manually set the channel
- **Random Selection** – The router randomly sets the channel
- **Smart Selection** (Default) – Scans to determine the lowest interference WiFi channel

Channel Selection Schedule: When using the "Smart" channel selection, this controls whether the router will periodically rescan for a better channel and change to it. Select from "Once," "Daily," "Weekly," or "Monthly." Note that there may be a momentary WiFi disconnection while the channel changes.

Channel: (Shows if **User Selection** is selected.) The WiFi channel* corresponds to a frequency the router uses to communicate with other devices. For 2.4 GHz, the range is 1 to 11, and 1, 6, and 11 do not overlap each other. Select a channel from the dropdown list:

- 1 (2412 MHz)
- 2 (2417 MHz)
- 3 (2422 MHz)
- 4 (2427 MHz)
- 5 (2432 MHz)



©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- 6 (2437 MHz)
- 7 (2442 MHz)
- 8 (2447 MHz)
- 9 (2452 MHz)
- 10 (2457 MHz)
- 11 (2462 MHz)

** - Channels listed above represent US/FCC settings. EU users will see different settings.*

Client Timeout: If the access point is not able to communicate with the client it will disconnect it after this timeout (in seconds).

TX Power: Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

RTS Threshold: When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value.

Fragmentation Threshold: Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value. Setting the Fragmentation value too low may result in poor performance.

DTIM: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

Beacon: Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000 milliseconds.

WPS: WiFi Protected Setup is a method for easy and secure establishment of a wireless network. It can be used instead of passwords when connecting clients that support WPS. To initiate WPS, either press the WPS button on the product (if it has one) or use the Connect button in the Getting Started / WiFi Protected Setup menu.

Short Slot: Slot Time is the period wireless clients use in determining if the channel is free for transmission. Enabling this value allows clients that can utilize a shorter time to do so. Disabling this option forces all clients to use a longer backoff check and thus may reduce network throughput while reducing the number of transmission collisions.

Wireless Mode: Select the WiFi clients with which the router will be compatible. Greater compatibility is a tradeoff with better performance. For greatest compatibility with all WiFi devices, select 802.11 a/b/g/n or 802.11 a/b/g/n/ac.

2.4 GHz options

- 802.11 b
- 802.11 b/g
- 802.11 a/b/g/n
- 802.11 b/g/n
- 802.11 n

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Channel Width: Selects whether the router uses a single 20 MHz channel to send/receive, or uses two adjacent 20 MHz channels to create a 40 MHz channel. Higher performance is possible with the 40 MHz channel. Selecting Auto is generally best. Enabling WiFi as WAN will force 20 MHz only mode.

Extended Channel: When operating in 40 MHz mode the access point will use an extended channel either below or above the current channel. Optimal selection will depend on the channels of other networks in the area.

MCS: 802.11n uses multiple Modulation Coding Schemes to enable higher throughput in various environments. Since clients can dynamically change rates depending on environment, selecting **Auto** is generally best.

Short GI: Short GI is an optimization for shortening the interval between transmissions. May be incompatible with older clients.

Greenfield Mode: Greenfield mode uses an 802.11n-only preamble to transmit packets which older wireless clients cannot interpret. Use of greenfield mode in a mixed 802.11 environment may result in degraded performance but can improve performance if all devices in the area are 802.11n compatible.

RADIUS Timeout: (Default: 3600 seconds) When using an Enterprise security mode clients will be forced to re-authenticate with the RADIUS server at this interval in seconds. This allows administrators to revoke access so when an attached client's authentication expires, the client must re-authenticate.

RADIUS Retry: (Default: 60 seconds) When using an Enterprise security mode, if a RADIUS query fails to receive a response from the server it will delay by this interval (in seconds) before attempting another query. This helps protect the network from floods of authentication requests if the RADIUS server is temporarily unreachable.

ETHERNET PORTS

Ethernet Port Configuration provides controls for your router's Ethernet ports. There are two ports: by default, one WAN port and one LAN port. While default settings will be sufficient in most circumstances, you have the ability to control: **Mode** (WAN or LAN) and **Link Speed**. Additional controls for WAN ports are available in **CONNECTION MANAGER**.

Mode: WAN or LAN. By default there is one LAN (Local Area Network) port and one WAN (Wide Area Network) port.

- **Internet (WAN)** is used as a possible source of Internet for the router
- **Local Network (LAN)** is for connecting a computer or similar device directly to the router with an Ethernet cable.

Link Speed: Default setting is Auto. The Auto setting is preferred in most cases.

- Auto
- 10Mbps - Half Duplex
- 10Mbps - Full Duplex
- 100Mbps - Half Duplex
- 100Mbps - Full Duplex
- 1000Mbps - Full Duplex

HOTSPOT SERVICES

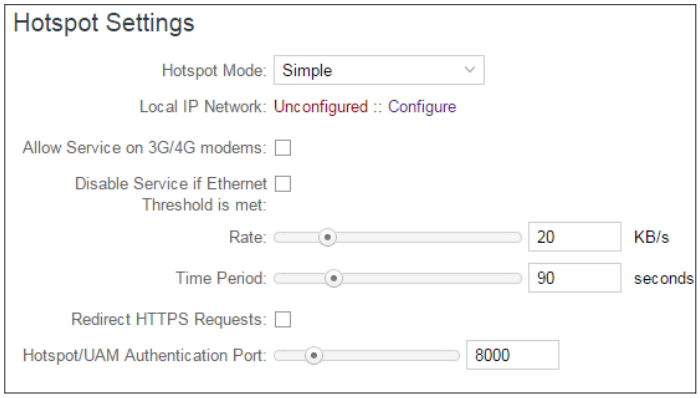
Any of your networks can be enabled as a hotspot. To enable a hotspot, you need to select a network and set it as a hotspot in **NETWORKING > Hotspot Services**.

NOTE: Although any network can be a hotspot, the router allows only one hotspot.

Hotspot Mode: Choose from the following dropdown options:

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- **Simple**: Allows "Terms of Use" page and timeout settings controlled within the router
- **RADIUS/UAM**: Allows you to set up external authentication servers


Hotspot Settings
Hotspot Mode: Simple
Local IP Network: Unconfigured :: Configure
Allow Service on 3G/4G modems:
Disable Service if Ethernet Threshold is met:
Rate: 20 KB/s
Time Period: 90 seconds
Redirect HTTPS Requests:
Hotspot/UAM Authentication Port: 8000

Local IP Network: A single LAN Group – including both WiFi and Ethernet – can be configured as your hotspot. If you do not already have a LAN Group configured as a hotspot, click **Configure** and set the **IPv4 Routing Mode** to "Hotspot" for the LAN Group you want to use.

NOTE: Routing Mode is in the Primary LAN Editor under the IPv4 Settings tab. Select a network in **NETWORKING > Local IP Networks** and click **Edit** to open the Primary LAN Editor.

Allow Service on 3G/4G Modems: Allows you to enable or disable hotspot access to the Internet over a modem. This is often used if the router has a main wired link and a secondary modem for failover (typically with a more expensive/limited data plan). Select this option if you want the router to allow data traffic over the modem if the wired connection goes down.

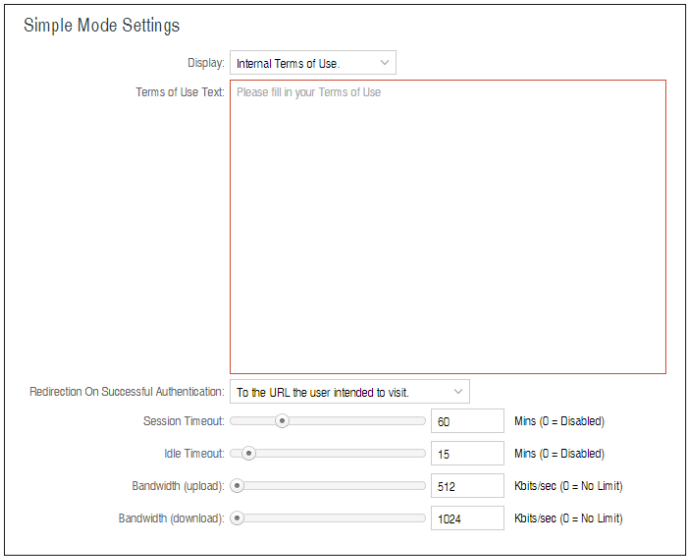
Disable Service if Ethernet Threshold is met: This will block hotspot use of the WAN when the threshold is met. This can be used if the router is being used as a backup failover connection to another router with a wired connection. If that other router's wired connection goes down and it starts using this router for its primary connection, then disable hotspot use of the WAN connection. Set the limiting **Rate** (KB/s) and **Time Period** (seconds).

Redirect HTTPS Requests: This allows initial requests to HTTPS websites to be redirected appropriately.

Hotspot/UAM Authentication Port: Default: 8000. Type in a different port number, or use the slider to change the port.

Simple Mode Settings

Display: This section allows you to choose if a "Terms of Use" page will be given to the user connecting to the hotspot.


Simple Mode Settings
Display: Internal Terms of Use.
Terms of Use Text: Please fill in your Terms of Use
Redirection On Successful Authentication: To the URL the user intended to visit.
Session Timeout: 60 Mins (0 = Disabled)
Idle Timeout: 15 Mins (0 = Disabled)
Bandwidth (upload): 512 Kbits/sec (0 = No Limit)
Bandwidth (download): 1024 Kbits/sec (0 = No Limit)

- **Internal Terms of Use**. Fill in your own terms of use.
- **External Terms of Use**. Specify a URL that has the Terms of Use page. Users will automatically be directed to this page.
- **No Terms of Use. Redirect Only**.

Redirection on Successful Authentication: Depending on your choice for the "Terms of Use" page, your have further options for where the user will be directed. After the user accepts the terms, you can either let him/her continue to the URL they were trying to reach or you can force the user to go to a specified URL once before continuing on.

- To the URL the user intended to visit
- To an administrator-defined URL

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Redirect URL: If you have chosen to send users to an administrator-defined URL, you will need to specify the address.

Session Timeout: (Default: 60 minutes.) The amount of time the user may use the router before being forced to authenticate again.

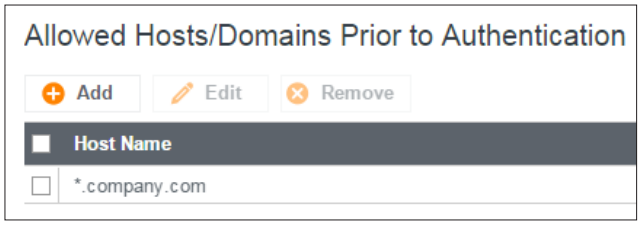
Idle Timeout: (Default: 15 minutes.) If the user is idle for this amount of time, make them re-authenticate.

Bandwidth (upload): (Default: 512 Kbits/sec.) The data rate limit for users uploading data through the hotspot.

Bandwidth (download): (Default: 1024 Kbits/sec.) The data rate limit for users downloading data through the hotspot.

Allowed Hosts/Domains Prior to Authentication

Adding hostnames to this list will allow access from your network to any external domain or website prior to being authenticated. For example, a hotel might allow access to its own website prior to authentication.



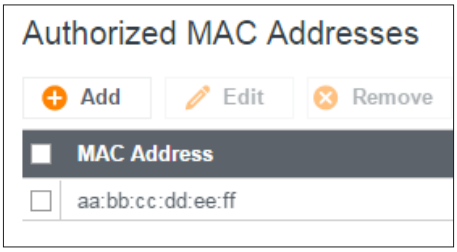
Click **Add** to enter new hostnames you wish to allow.

Enter the hostname or domain name of the website you wish to **allow**, e.g. www.company.com or company.com. To allow all domain and sub-domain options, use a wildcard, e.g. *.company.com.

Click **Update** to save your additions.

Authorized MAC Addresses

Add the MAC addresses of trusted machines. This gives them automatic access through the hotspot portal.



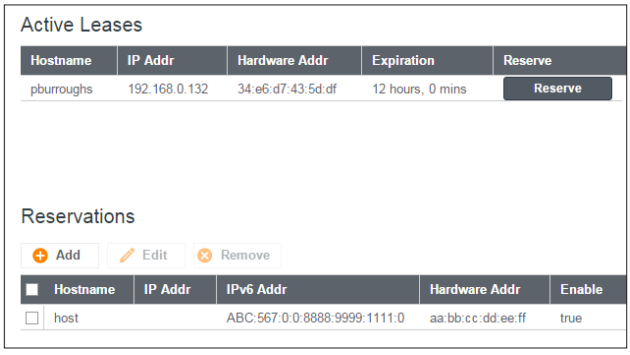
Click **Add** to enter new MAC Addresses you wish to allow.

Click **Update** to save your additions.

DHCP SERVER

DHCP stands for Dynamic Host Configuration Protocol. The built-in DHCP server automatically assigns IP addresses to the computers and other devices on each local area network (LAN). In this section you can view a list of assigned IP addresses and reserve IP addresses for particular devices.

Active Leases: A list of devices that have been provided DHCP leases. The DHCP server automatically assigns these leases. This list will not include any devices that have static IP addresses on the network. Select a device and click **Reserve** to add the device and its IP address to the list of **Reservations**.



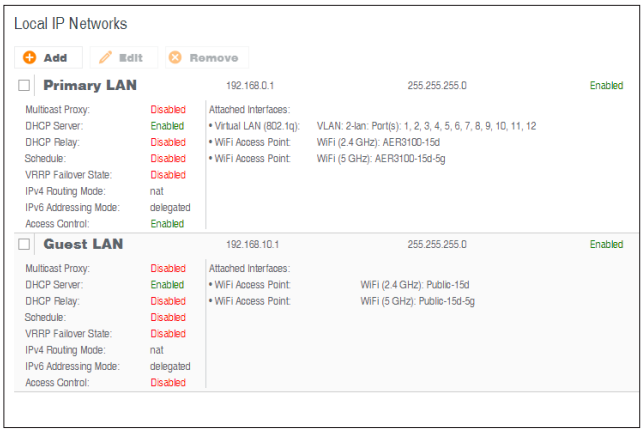
Reservations: This is a list of devices with reserved IP addresses. This reservation is almost the same as when a device has a static IP address except that the device must still request an IP address from the router. The router will provide the device the same IP address every time. DHCP reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or a reservation.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

While you have the option to manually input the information to reserve an IP address (Hostname, Hardware Addr, IP Addr), it is much simpler to select a device under the **Active Leases** section and click "**Reserve**." The selected device's information will automatically be added under **Reservations**.

LOCAL IP NETWORKS

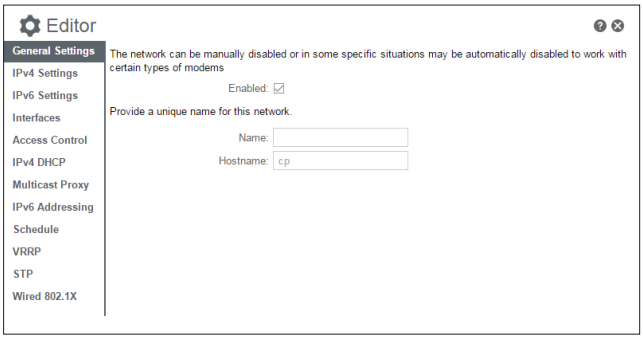
Local IP Networks displays the following information for each network:



- **Network Name**, **IP address/Netmask**, and **Enabled/Disabled** (along the top bar)
- **Multicast Proxy** (Enabled/Disabled)
- **DHCP Server** (Enabled/Disabled)
- **DHCP Relay** (Enabled/Disabled)
- **Schedule** (Enabled/Disabled – See the Schedule tab in the Local Network Editor)
- **VRRP Failover State** (Disabled, Backup, or Master)
- **IPv4 Routing Mode** (NAT, Standard, IP Passthrough, Hotspot, Disabled)
- **IPv6 Addressing Mode** (SLAAC Only, SLAAC with DHCP, Disable SLAAC and DHCP)
- **Access Control** (Admin Access, UPnP Gateway, LAN Isolation)
- **Attached Interfaces** (Ethernet ports, WiFi, VLAN)

Click **Add** to configure a new network, **Remove** to delete a network, or select an existing network and click **Edit** to view configuration options.

General Settings



Enabled: The network can be manually disabled or in some specific situations may be automatically disabled to work with certain types of modems.
Name: The "name" property primarily helps to identify this network during other administration tasks.
Hostname: The hostname is the DNS name associated with the router's local area network IP address.

IPv4 Settings

IP Address: This is the address used by the router for local area network communication. Changes to this parameter may require a restart to computers on this network.
Netmask: The netmask controls how many IP addresses can be used in this network. The default value is usually acceptable for most situations.
IPv4 Routing Mode: Each network can use a unique routing mode to connect to the Internet. The default of NAT is desirable in most configurations.

- **NAT:** Network Address Translation hides private IP addresses behind the router's IP address.
- **Standard:** Without NAT exposes the subnet addresses which requires them to be externally routable.
- **IP Passthrough:** IP Passthrough passes the IP address given by the modem WAN through the router. Hotspot, VPN, and GRE must be disabled. Any Wireless interfaces must be removed from this network in order to enable IP Passthrough.
- **Hotspot:** Provide Hotspot Services on this Network, requiring Terms of Service or RADIUS/UAM authentication before WAN access will occur on both Wireless and Wired LAN connections.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

IPv6 Settings

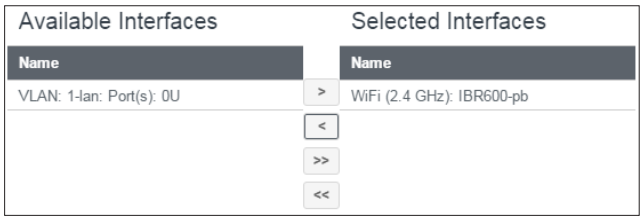
IPv6 Address Source: The Address source has three settings. The default of **Delegated** is desirable in most configurations.

- **Delegated:** The address is provided by a router connected to this router's WAN.
- **Static:** The address is provided by the router admin.
- **None:** No use of an IPv6 WAN address, IPv6 is disabled on the WAN.

IPv6 Address: An IPv6 Address is a unique numerical label for a computer or device using the Internet Protocol (IP). IPv6 addresses are typically in the format composed of 8 sets of 4 hexadecimal numbers. Leading zeros can be ignored and the longest set of continuous zeros can be replaced with **::**. For example, the IPv6 address of 0001:0000:0234:5678:0000:0000:9abc:0def can be expressed as 1:0:234:5678**::**9abc:def.

Interfaces

Select the network interfaces which will be attached to this network by either dragging desired interface or clicking left or right arrows to move them between **Available Interfaces** and **Selected Interfaces**.

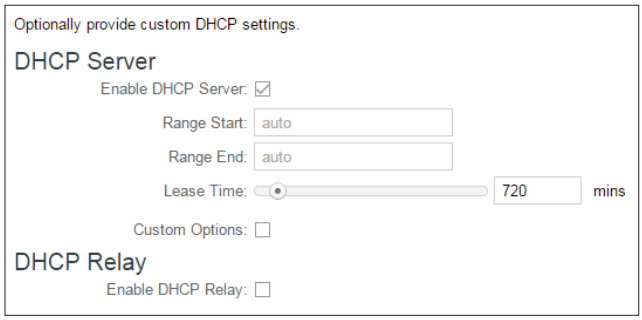


Access Control

UPnP Gateway: Select the UPnP (Universal Plug and Play) option if you want to enable the UPnP Gateway service for computers on this network.
Admin Access: When enabled users may access these admin pages from this network.

IPv4 DHCP

DHCP Server



- **Enable DHCP Server:** When the DHCP server is enabled, users of your network will be able to automatically connect to the Internet without any special configuration. It is recommended that you leave this enabled. Advanced DHCP server configuration is available at **NETWORKING > Local Networks > DHCP Server**.
- **Range Start:** The starting IP address in the DHCP Server range is the beginning of the reserved pool of IP addresses which will be given to any DHCP enabled computers on your network. The default value is almost always sufficient.
- **Range End:** The ending IP address in the DHCP Server range is the end of the reserved pool of IP addresses which will be given to any DHCP enabled computers on your network. The default value is almost always sufficient.
- **Lease Time:** The lease time specifies how long DHCP enabled computers will wait before requesting a new DHCP lease. Smaller values are better suited to busy environments.
- **Custom Options:** Send optional extra options to DHCP clients of this network. This can be used to, for example, set the boot TFTP server of a network for disk-less clients.

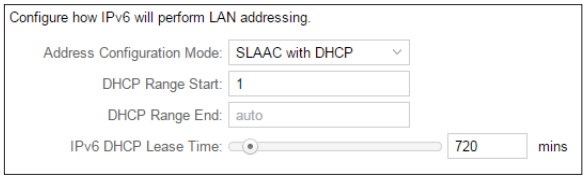
DHCP Relay

- **Enable DHCP Relay:** DHCP Relay communicates with a DHCP server and acts as a proxy for DHCP broadcast messages that must be routed to remote segments. This is accomplished by converting broadcast DHCP messages to unicast messages to communicate between clients and servers.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Multicast Proxy
Multicast Proxy: Enables IGMP proxying to allow Multicast Streams to flow across this network.
Quick Leave Mode: Disable quick leave mode if it's vital that the daemon should act exactly as a real multicast client on the upstream interface. However, disabling this function increases the risk of bandwidth saturation.
Altnet: If multicast traffic originates outside the upstream subnet, add address(es) to the "altnet" to define legal multicast sources.

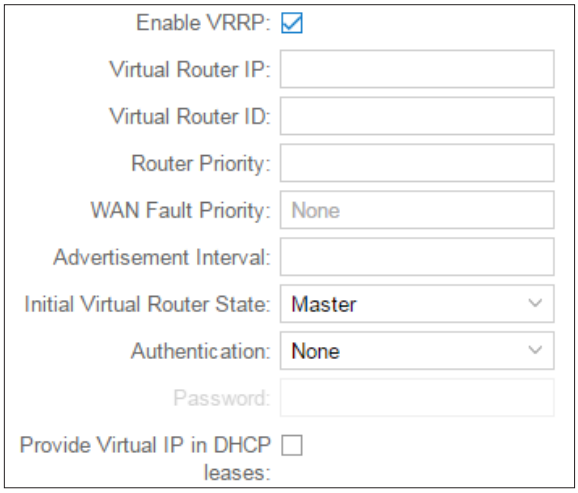
IPv6 Addressing
Address Configuration Mode: SLAAC stands for Stateless address autoconfiguration. A network can be configured to use SLAAC only, or it can be configured to also use DHCPv6 to provide ip addresses to clients.
DHCP Range Start: The DHCP Range Start is the beginning of the range that will be used for IPV6 DHCP addresses. The IPv6 range will always start at 1.



DHCP Range End: The ending IP address in the DHCP Server range is the end of the reserved pool of IP addresses which will be given to any DHCP enabled computers on your network.
IPv6 DHCP Lease Time: Specifies how long DHCP enabled computers will wait before requesting a new DHCP lease.

Schedule
Enable Schedule Service: Enable the interface scheduler. A schedule allows an interface to be enabled or disabled during specific hours of a day.

VRRP
Enable VRRP: Enable or disable VRRP.
Virtual Router IP: IP Address of the Virtual Router.
Virtual Router ID: Identifier of the Virtual Router.
Router Priority: Failover priority of this router. The highest priority router will take ownership of the Virtual IP.
WAN Fault Priority: This optional value sets the failover priority of this router when no WAN connection is available. If the value matches the normal router priority, WAN connection state will not be considered. If the value is empty (the default), the router will always give up the Virtual IP and let a new master take over when no WAN connection is available.
Advertisement Interval: Sets the amount of time (in seconds) between sending VRRP advertisements.
Initial Value Router State: This controls the initial failover state of the VRRP instance when it first comes up.
Authentication: VRRP Authentication Method. Note that VRRP Authentication has been deprecated as of RFC 3768.



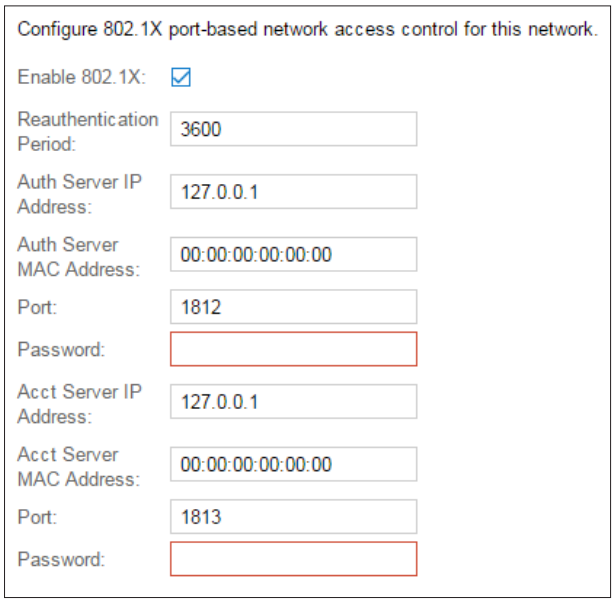
Password: VRRP Group Password.
Provide Virtual IP in DHCP leases: Select this to automatically set the DHCP default gateway address and DNS server address to the Virtual IP in DHCP leases provided on this network.

STP
Enable STP: Enable **Spanning Tree Protocol** loop detection.
Bridge Priority: Set the priority of the bridge. When determining the root bridge of the spanning tree topology, the bridge priority is compared first. The bridge with the lowest priority with will win. If you want this router to

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

be the root bridge, then set it to a value less than the default of 32768. A valid priority value is between 0 and 65535.

Wired 802.1X

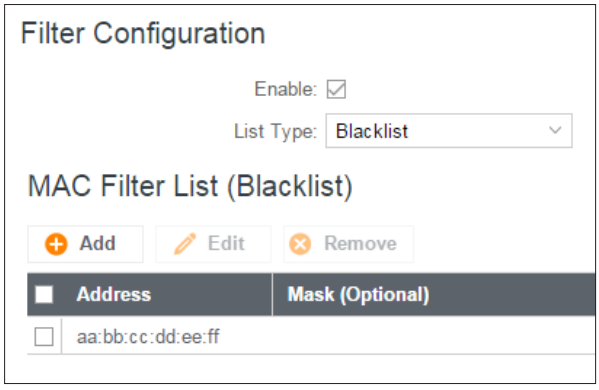


Enable 802.1X: Require IEEE 802.1X Authorization.
Reauthentication Period: EAP reauthentication period in seconds.
Auth Server IP Address: IP address of the connected RADIUS server.
Auth Server MAC Address: Hardware address of the connected RADIUS server's interface. *NOTE: If you don't know the MAC address for the RADIUS server, enter 00:00:00:00:00:00, and the service will try to find the MAC address from the given IP address.*
Port
Password
Acct Server IP Address: IP address of the connected RADIUS server.
Acct Server MAC Address: This is the Hardware address of the connected RADIUS server's interface. *NOTE: If you don't know the MAC address for the RADIUS server, enter 00:00:00:00:00:00, and the service will try to find the MAC address from the given IP address.*
Port
Password

MAC FILTER & LOGGING

A MAC (Media Access Control) address is a unique identifier for a computer or other device. This page allows you to manage clients by MAC address. You can filter clients by MAC addresses and/or keep a log of devices connected to your router.

Filter Configuration



The MAC Filter allows you to create a list of devices that have either exclusive access (whitelist) or no access (blacklist) to your local network.

Enabled: Click to allow MAC Filter options.
Whitelist: Select either "Whitelist" or "Blacklist" from a dropdown menu. In "Whitelist" mode, the router will restrict LAN access to all computers except those contained in the "MAC Filter List" panel. In "Blacklist" mode, listed devices are completely blocked from local network access.

MAC Filter List (Whitelist or Blacklist)
Add devices to either your whitelist or blacklist simply by inputting each device's MAC address.

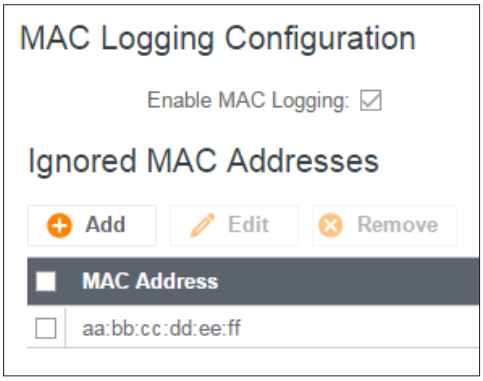
NOTE: Use caution when using the MAC Filter to avoid accidentally blocking yourself from accessing the router.

MAC Logging Configuration
Enable MAC Logging: Enabling MAC Logging will cause the router to log MAC addresses that are connected

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

to the router. MAC addresses that you do not want to have logged (addresses that you expect to be connected) should be added to the "Ignored MAC Addresses" list.

You can configure the router to send an alert if a connected device has a MAC address that the router doesn't recognize. Go to **SYSTEM > Device Alerts** to set up these email alerts.



Ignored MAC Addresses
This is the list of MAC addresses that will not produce an alert or a log entry when they are connected to the router. These should be MAC addresses that you expect to be connected to the router. To add MAC addresses to this list, simply select devices shown in the MAC Address Log and click "Ignore." You can also add addresses manually.

MAC Address Log
This shows the last 64 MAC addresses that have connected to the router, as well as which interface was used to connect. The time/date that is logged is the time of the first connection. The page may need to be refreshed to show the most recent log entries.

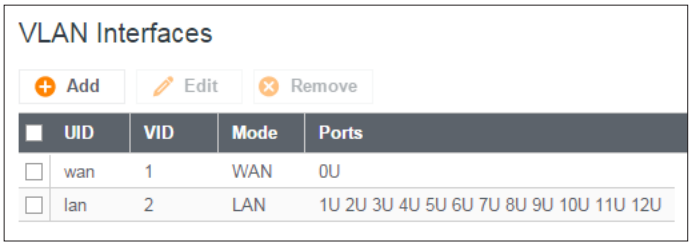
Double-clicking on entries from this list will add them to the **Ignored MAC Addresses** list.

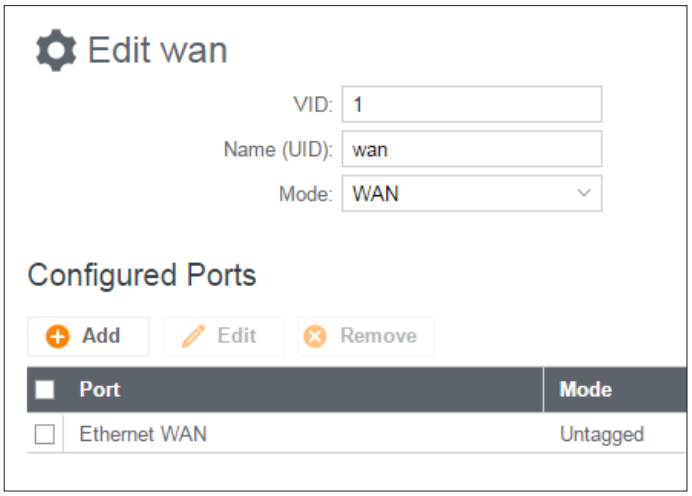
VLAN INTERFACES

A virtual local area network, or VLAN, functions as any other physical LAN, but it enables computers and other devices to be grouped together even if they are not physically attached to the same network switch.

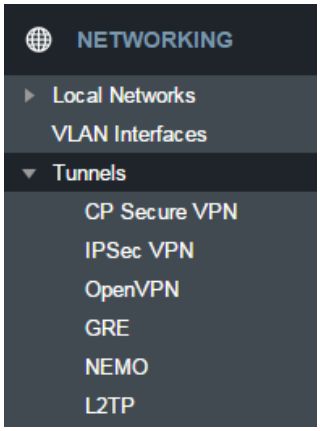
To enable a VLAN, select a VID (virtual LAN ID) and a group of Ethernet ports through which users can access the VLAN. Then go back up to the **Local Network Editor** to attach your new VLAN to a network. To use a VLAN, the VID must be shared with another router or similar device so that multiple physical networks have access to the one virtual network.

Click **Add** to create a new VLAN interface. To edit an interface, select the check box next to the desired interface.





©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com



TUNNELS

CP SECURE VPN

Configured, deployed, and managed from the cloud, CP Secure VPN delivers a virtual private data network that minimizes both cost and complexity. Unlike traditional bulky head-end concentrator hardware solutions, CP Secure VPN allows IT managers to secure their expanding Edge Networks using architectures that scale quickly and are easy to maintain. For more information, visit **cradlepoint.com**.

NOTE: CP Secure VPN requires an NCM Prime subscription. For more information, visit **cradlepoint.com**.

IPSEC VPN

VPN (virtual private network) tunnels are used to establish a secure connection to a remote network over a public network. For example, VPN tunnels can be used across the Internet by an individual to connect to an office network while traveling, or by two office networks to function as one network. The two networks set up a secure connection across the (normally) unsecure Internet by assigning VPN encryption protocols.

Cradlepoint VPN tunnels use **IPsec** (Internet Protocol security) to authenticate and encrypt packets exchanged across the tunnels. To set up a VPN tunnel with a Cradlepoint router on one end, there must be another device (usually a router) that also supports IPsec on the other end.

IKE (Internet Key Exchange) is the security protocol in IPsec. IKE has two phases, phase 1 and phase 2. The router has several different security protocol options for each phase, but the default selections will be sufficient for most users.

The VPN tunnel status page allows you to view the state of the VPN tunnels. If a tunnel fails to connect to the remote site, check the System Logs for more information. You may double click on a cell to directly edit that information.

Click **Add** to configure a new VPN tunnel; click **Edit** to make changes to an existing tunnel.

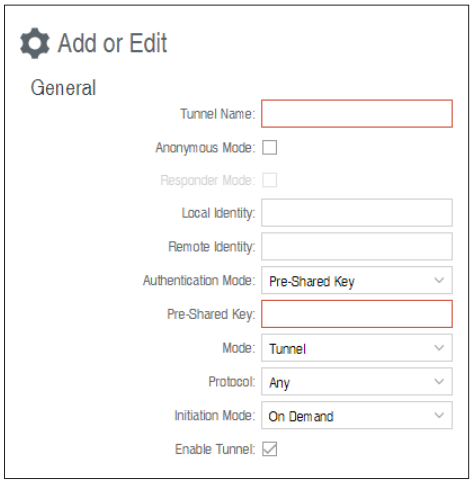
Add/Edit Tunnel – General

Tunnel Name: Give the tunnel a name that uniquely identifies it.

Anonymous Mode: Select to allow remote connections from any IP address.

Responder Mode: When enabled, the router will not initiate negotiation with peers.

Local Identity: Specifies the identifier sent to the remote host during phase 1 negotiation. If left blank it will default to the IP address of the WAN connection. Currently we only support identifiers in the form of an IP address, a user-fully qualified domain name (user@mydomain.com) or just a fully qualified domain name (www.mydomain.com). If the remote side of the tunnel is configured to expect an identifier, then both must match in order for the negotiation to succeed. If NAT-T is being used, a single word (instead of an address) can be used if a DynDNS connection is not being used.



©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Remote Identity: Specifies the identifier we expect to receive from the remote host during phase 1 negotiation. If no identifier is defined then no verification of the remote peer's identification will be done. Currently we only support identifiers in the form of an IP address, a user-fully qualified domain name (user@mydomain.com) or just a fully qualified domain name (www.mydomain.com). If left blank we will default to the IP address of the WAN connection. If NAT-T is being used, a single word (instead of an address) can be used if a DynDNS connection is not being used.

Authentication Mode: Select from **Pre-Shared Key** and **Certificate**. **Pre-Shared Key** is used when there is a single key common to both ends of the VPN. **Certificate** requires the creation of a set of certificates and a private key that can be uploaded to the router. Select **Enable Certificate Support** in the **Global VPN Settings** section to upload a single set of certificates for the router to use.

Pre-Shared Key: Create a password or key. The routers on both sides of the tunnel must use this same key.

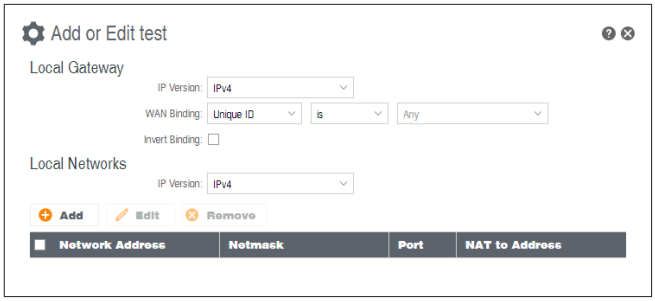
Mode: Select from **Tunnel**, **Transport** or **VTI-Tunnel**. **Tunnel Mode** is used for protecting traffic between different networks, when traffic must pass through an intermediate, untrusted network. **Transport Mode** is used for end-to-end communications (for example, for communications between a client and a server). **VTI Tunnel** creates a virtual tunnel interface with a specified virtual IP address. This interface can then be added to the zone firewall.

Initiation Mode: **Always On** or **On Demand**. **Always On** is used if you want the tunnel to initiate the tunnel connection whenever the WAN becomes available. Select **On Demand** if you want the tunnel to initiate a connection if and only if there is data traffic bound for the remote side of the tunnel.

Tunnel Enabled: Enabled or Disabled.

Add/Edit Tunnel – Local Gateway
IP Version: Select **IPv4** or **IPv6**.

WAN Binding: WAN Binding is an optional parameter used to configure the VPN tunnel to ONLY operate when the specified WAN device(s) are available and connected. An example use case is when there is a router with both a primary and failover WAN device and the tunnel should only be used when the system has failed over to the backup connection.



Make a selection for "When," "Condition," and "Value" to create a WAN Binding. The condition will be in the form of these examples:

When	Condition	Value
Port	Is	USB Port 1
Type	Is not	WiMax

- When:
  - **Port** – Select by the physical port on the router that you are plugging the modem into (e.g., "USB Port 2").
  - **Manufacturer** – Select by the modem manufacturer (e.g., "Cradlepoint Inc.").
  - **Model** – Set your rule according to the specific model of modem.
  - **Type** – Select by type of Internet source (Ethernet, LTE, Modem, Wireless as WAN, WiMAX).
  - **Serial Number** – Select a 3G or LTE modem by the serial number.
  - **MAC Address** – Select a WiMAX modem by MAC Address.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

  - **Unique ID** – Select by ID. This is generated by the router and displayed when the device is connected to the router.
- **Condition**: Select "is," "is not," "starts with," "contains," or "ends with" to create your condition's statement.
- **Value**: If the correct values are available, select from the dropdown list. You may need to manually input the value.

Invert Binding: Advanced option that inverts the meaning of WAN Binding to only establish this tunnel when the specified WAN Binding device(s) are *NOT* connected.

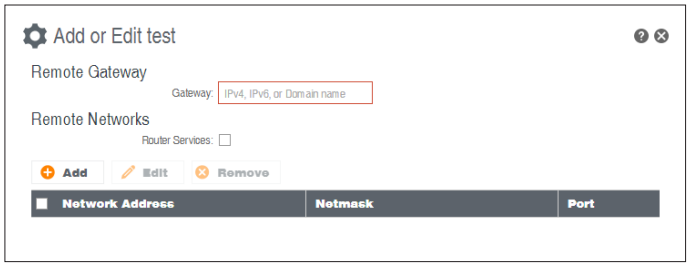
Add/Edit Tunnel – Local Networks
IP Version: Select **IPv4** or **IPv6**.

The **Network Address** and the **Netmask** define what local devices have access to or can be accessed from the VPN tunnel.

NOTE: the local network IP address MUST be different from the remote network IP address.

Optionally: A **Port** can be defined that will limit the traffic going through the VPN tunnel to only that port. If the field is left blank, any port will be accepted by the tunnel.

Add/Edit Tunnel – Remote Gateway
Gateway: This value can be any of the following: an IPv4 address, an IPv6 address, or a fully qualified name in the form of "host.domain.com" (DNS names are case-insensitive, so only lower case letters are allowed). It is recommended that you use a dynamic DNS hostname instead of the static IP address – by using the dynamic DNS hostname, updates of the remote WAN IP are compensated for while connecting to a VPN tunnel.



Add/Edit Tunnel – Remote Networks
The **Network Address** and the **Netmask** define the remote network address range that local devices will have access to via the VPN tunnel.

NOTE: the remote network IP address *MUST* be different from the local network IP address.

Optionally: A **Port** can be defined that will limit the traffic going through the VPN tunnel to only that port. If the field is left blank, any port will be accepted by the tunnel.

Add/Edit Tunnel – IKE Phase 1
IKE security has two phases, phase 1 and phase 2. You have the ability to distinctly configure each phase, but the default settings will be sufficient for most users.

To set up a tunnel with a remote site, you need to match your tunnel's IKE negotiation parameters with the remote site. By selecting several encryption, hash, and DH group options, you improve your chances for a successful tunnel negotiation. For greatest compatibility, select all options; for greatest security, select only the most secure options that your devices support.

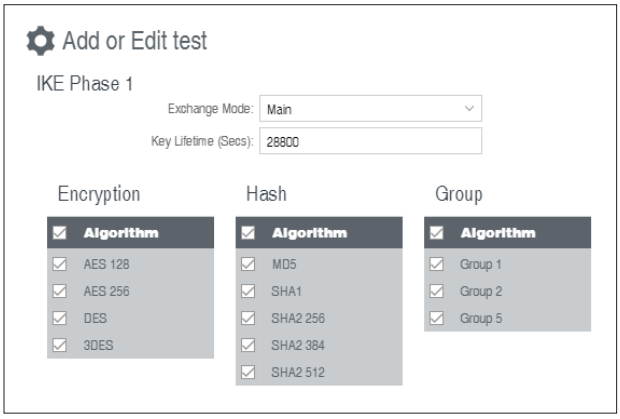
Exchange Mode: The IKE protocol has two modes of negotiating phase 1 – **Main** (also called Identity Protection) and **Aggressive**.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- In **Main** mode, IKE separates the key information from the identities, allowing for the identities of peers to be secure at the expense of extra packet exchanges.
- In **Aggressive** mode, IKE tries to combine as much information into fewer packets while maintaining security. Aggressive mode is slightly faster but less secure.

Because it has better security, **Main** mode is recommended for most users.

Key Lifetime: The lifetime of the generated keys of phase 1 of the IPsec negotiation from IKE. After the time has expired, IKE will renegotiate a new set of phase 1 keys.



Encryption, Hash, and DH Groups
Each IKE exchange uses one encryption algorithm, one hash function, and one DH group to make a secure exchange.

Encryption: Used to encrypt messages sent and received by IPsec.

- AES 128
- AES 256
- DES
- 3DES

Hash: Used to compare, authenticate, and validate that data across the VPN arrives in its intended form and to derive keys used by IPSec.

- MD5
- SHA1
- SHA2 256
- SHA2 384
- SHA2 512

Note that some Encryption/Hash combinations (e.g., 3DES with SHA2 384/512) are computationally expensive, impacting WAN performance. AES is as strong an encryption and performs much better than 3DES.

DH Groups: The DH (Diffie-Hellman) Group is a property of IKE and is used to determine the length of prime numbers associated with key generation. The strength of the key generated is partially determined by the strength of the DH Group. Group 5, for instance, has greater strength than Group 2.

- Group 1: 768-bit key
- Group 2: 1024-bit key
- Group 5: 1536-bit key

In IKE Phase 1 you can only select one DH group if you are using **Aggressive** exchange mode.

By default, all the algorithms (encryption, hash, and DH groups) supported by the device are checked, which means they are allowed for any given exchange. Deselect these options to limit which algorithms will be accepted. Be sure to check that the router (or similar device) at the other end of the tunnel has matching algorithms.

The algorithms are listed in order by priority. You can reorder this priority list by clicking and dragging algorithms up or down. Any selected algorithm may be used for IKE exchange, but the algorithms on the top of the list are more likely to be used more often.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Add/Edit Tunnel – IKE Phase 2

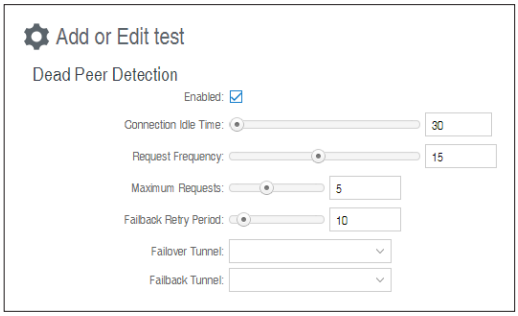
Perfect Forward Secrecy (PFS): Enabling this feature will require IKE to generate a new set of keys in phase 2 rather than using the same key generated in phase 1. Additionally, with this option enabled the new keys generated in phase 2 are exchanged in an encrypted session. Enabling this feature affords the policy greater security.

Key Lifetime: The lifetime of the generated keys of phase 2 of the IPsec negotiation from IKE. After the time has expired, IKE will renegotiate a new set of phase 2 keys.

Phase 2 has the same selection of **Encryption** and **DH Groups** as phase 1, but you are restricted to only one DH Group. Phase 2 and phase 1 selections do not have to match. For the **Hash** selection an added value of SHA 256_128 (128-bit truncation) is avaliable. The original specification and the Cradlepoint default is 96-bit truncation, but RFC4868 requires 128-bit. A VPN to newer Cisco or Juniper devices will typically require 128-bit.

Add/Edit Tunnel – Dead Peer Detection

Dead Peer Detection (DPD) defines how the router will detect when one end of the IPsec session loses connection while a policy is in use.



Connection Idle Time: Configure how long the router will allow an IPsec session to be idle before beginning to send Dead Peer Detection (DPD) packets to the peer machine. (Default: 30 seconds. Range: 10 – 3600 seconds.)

Request Frequency allows you to adjust the delay between these DPD packets. (Default: 15 seconds. Range: 2 – 30 seconds.)

Maximum Requests: Specify how many requests to send at the selected time interval before the tunnel is considered dead. (Default: 5. Range: 2 – 10.)

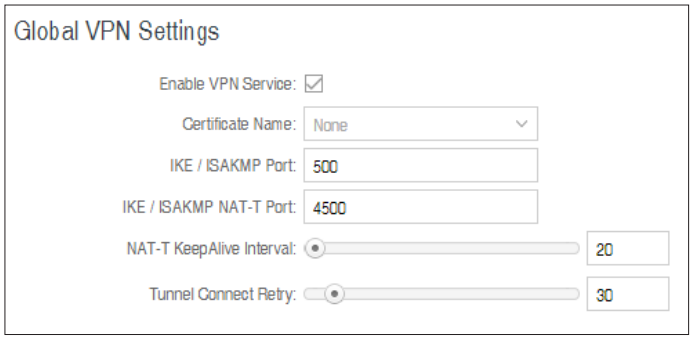
Failback Retry Period: If you have VPN tunnel failover/failback enabled (see below), set the time period between each check on the primary network after failover. (Default: 10 seconds. Range: 5 – 60 seconds.)

Failover Tunnel and **Failback Tunnel**: Use these settings to create two tunnels – one as the primary tunnel and one as the backup tunnel. To configure tunnel failover/failback, complete the following steps:

1. Create two tunnels: one for primary and one for backup. Make sure that both tunnels have the same **Remote Network** and that both have **Dead Peer Detection** enabled.
2. Choose one to be the primary tunnel. Open the editor for this tunnel and make sure **Tunnel Enabled** is selected. Then go to the **Dead Peer Detection** page. Under **Failover Tunnel** select the other tunnel you have created.
3. Open the editor for the failover tunnel. Make sure **Tunnel Enabled** is *not* selected. On the **Dead Peer Detection** page, set the **Failback Tunnel** to your primary tunnel.

Global VPN Settings

These settings apply to all configured VPN tunnels.



Enable VPN Service: Enabling VPN Service will allow you to load a certificate for VPN to the router.

Certificate Name: Select the Certificate Name.

IKE / ISAKMP Port: Internet Key Exchange / Internet Security Association and Key Management Protocol port. (Default: 500. This is a standard VPN port that usually does not need to be changed.)

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

IKE / ISAKMP NAT-T Port: Internet Key Exchange / Internet Security Association and Key Management Protocol network address translation traversal port. (Default: 4500. This is a standard VPN NAT-T port that usually does not need to be changed.)

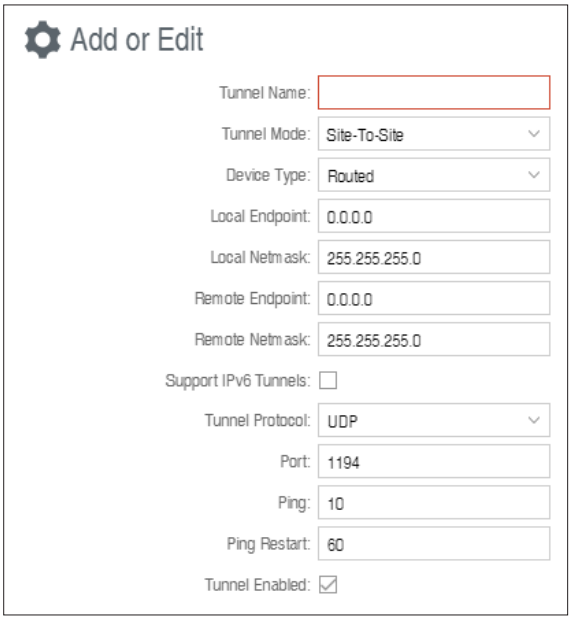
NAT-T KeepAlive Interval: Number of seconds between sending NAT-T packets to keep the tunnel alive if no other traffic is being sent. (Default: 20 seconds. Range: 0-3600 seconds. 20 seconds will be sufficient in almost all cases.)

Tunnel Connect Retry: Number of seconds between connection attempts. (Default: 30 seconds. Range: 10-255 seconds. 30 seconds will be sufficient in almost all cases.)

OPEN VPN (ONLY ON IBR600)

OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

Once you have a valid feature license, click **Add** to create a new OpenVPN tunnel. Click **Edit** to make changes to an existing tunnel.



Add/Edit Tunnel – General

- **Tunnel Name** – Enter a name to uniquely identify this tunnel
- **Tunnel Mode** – Select which mode this tunnel endpoint is required to be. Choose from the following:
  - Client
  - Server
- **Device Type -** Select between Routed (TUN) or Bridged (TAP) virtual device.
  - **Routed** creates an interface that can be used in the Zone Firewall and is fully routable.
  - **Bridged** creates a network interface that can be assigned to a LAN under the Local Networks configuration. This interface is managed through the assigned LAN device.
- **Local Endpoint -** Enter the IP Address of the LNS (tunnel server) peer
- **Local Netmask** – Enter the Netmask of the LNS (tunnel server) peer
- **Remote Endpoint** – Enter the IP Address of the LNS (tunnel server) peer
- **Remote Netmask** – Enter the Netmask of the LNS (tunnel server) peer
- **Support IPv6 Tunnels** – Allow IPv6 traffic to be forwarded over this tunnel. If you select this option, also input an **IPv6 Tunnel Address** and **Tunnel Prefix Length** for IPv6
- **Tunnel Protocol** – Choose UDP or TCP
- **Port** – Specify the port if desired
- **Ping** – (Displays if the **Configuration Mode** is **Advanced**) If no packets have been sent in the amount of time entered, a ping is sent to the remote endpoint
- **Ping Restart** – (Displays if the **Configuration Mode** is **Advanced**) If no pings have been received in the amount of time entered, OpenVPN restarts the tunnel

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- **Tunnel Enabled** – Click to enable/disable this tunnel

Add/Edit Tunnel – Security

- **Cipher** – Encrypt packets with the selected algorithm. The default is BF-CBC, an abbreviation for Blowfish in Cipher Block Chaining mode. Blowfish has the advantages of being fast, very secure, and allowing key sizes of up to 448 bits. Blowfish is designed to be used in situations where keys are changed infrequently. OpenVPN supports the CBC, CFB, and OFB cipher modes, however CBC is recommended and CFB and OFB should be considered advanced modes.
- **Auth Algorithm** – Authenticate packets with HMAC using message digest algorithm alg. (The default is SHA1). HMAC is a commonly used message authentication algorithm (MAC) that uses a data string, a secure hash algorithm, and a key, to produce a digital signature.
- **Verify peer certificate** – Verifies that peer certificate was signed with RFC3280 TLS rules set in key usage and extended key usage. This helps to prevent specific man-in-the-middle attacks.
- **TLS-Authentication** – In client/server mode: adds an additional layer of HMAC authentication on top of the tls control channel to protect against DoS attacks. In point-to-point mode: encrypts the communication using a static key. These keys must match on each endpoint.

Add/Edit Tunnel – Remote Servers

Create a list of remote server connections to connect to. OpenVPN will try to connect to each host in the list. If a disconnect occurs from a given server, the next server will be tried in a round-robin fashion.

- **Host** – IP address of the remote server
- **Port** – Specify the port if desired
- **Protocol** – Select UDP or TCP

Add/Edit Tunnel – Routes

Add or remove the routes that will be used to direct packets through the tunnel.

- **Network Address**
- **Netmask**

Generate Client Configuration

The Generate Client Configuration button can be used to generate client configurations for OpenVPN tunnels configured in Server mode. An .ovpn file will be created that can be imported to a variety of OpenVPN client devices (Android, iOS, Windows). If the private key for the server's certificate authority is known, a client certificate can be generated; otherwise one can be selected.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

GRE

Generic Routing Encapsulation (GRE) tunnels can be used to create a connection between two private networks. Most Cradlepoint routers are enabled for both GRE and VPN tunnels. GRE tunnels are simpler to configure and more flexible for different kinds of packet exchanges, but VPN tunnels are much more secure.

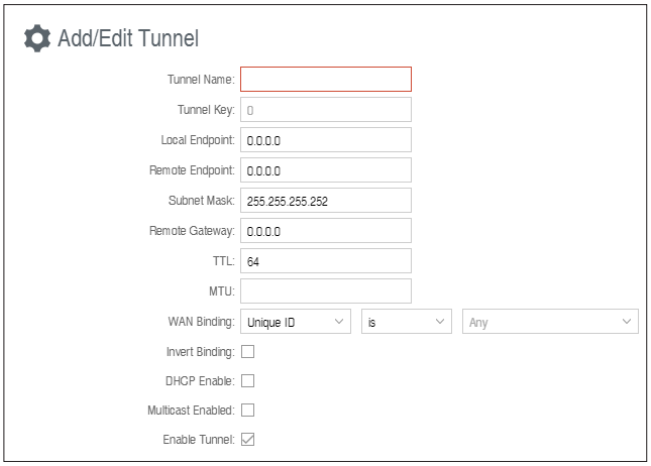
In order to set up a tunnel you must configure the following:

- **Local Network** and **Remote Network** addresses for the "**Glue Network**," the network that is created by the administrator that serves as the "glue" between the networks of the tunnel. Each address must be a different IP address from the same private network, and these addresses together form the endpoints of the tunnel.
- **Remote Gateway**, the public facing WAN IP address that the local gateway is going to connect to.
- **Routes** that allow you to configure what network traffic from local host(s) will be allowed through the tunnel.

Optionally, you might also want to enable the tunnel **Keep Alive** feature to monitor the status of a tunnel and more accurately determine if the tunnel is alive or not.

Click **Add** to configure a new GRE tunnel; click **Edit** to make changes to an existing tunnel.

Add/Edit Tunnel – General



Tunnel Name: Give the tunnel a name that uniquely identifies it.
Tunnel Key: Enables an ID key for a GRE tunnel, which can be used as an identifier for mGRE (Multipoint GRE).
Local Network: This is the local side of the "Glue Network," a network created by the administrator to form the tunnel. The user creates the IP address entered here. It must be different from the IP addresses of the networks it is gluing together. Choose any private IP address from the following three ranges that doesn't match either network:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Remote Network: This is the remote side of the "Glue Network." Again, the user must create an IP address that is distinct from the IP addresses of the networks that are being glued together.
The Remote Network and Local Network values will be flipped when input for the other side of the tunnel configuration.

Subnet Mask: This is the subnet mask for the Glue Network. The Local and Remote Network addresses must fit with this mask. 255.255.255.0 is a logical choice for most users.

Remote Gateway: This is the public facing, WAN-side IP address of the network to which the local gateway is going to connect.

TTL: Set the Time to Live (**TTL**), or *hop limit*, for the GRE tunnel.

MTU: Set the maximum transmission unit (**MTU**) for the GRE tunnel.

WAN Binding: WAN Binding is an optional parameter used to configure the GRE tunnel to *ONLY* operate when the specified WAN device(s) are available and connected. An example use case is when there is a router with both a primary and failover WAN device and the tunnel should only be used when the system has failed over to the backup connection.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Make a selection for "When," "Condition," and "Value" to create a WAN Binding. The condition will be in the form of these examples:

When	Condition	Value
Port	Is	USB Port 1
Type	Is not	WiMax

- **When**:
  - **Port** – Select by the physical port on the router into which you are plugging the modem (e.g., "USB Port 2").
  - **Manufacturer** – Select by the modem manufacturer (e.g., "Cradlepoint Inc.")
  - **Model** – Set your rule according to the specific model of modem
  - **Type** – Select by type of Internet source (Ethernet, LTE, Modem, Wireless as WAN, WiMAX)
  - **Serial Number** – Select a 3G or LTE modem by the serial number
  - **MAC Address** – Select a WiMAX modem by MAC Address
  - **Unique ID** – Select by ID. This is generated by the router and displayed when the device is connected to the router.
- **Condition**: Select "is," "is not," "starts with," "contains," or "ends with" to create your condition's statement.
- **Value**: If the correct values are available, select from the dropdown list. You may need to manually input the value.

Invert WAN Binding: Advanced option that inverts the meaning of WAN Binding to only establish this tunnel when the specified WAN Binding device(s) are *NOT* connected.

Tunnel Enabled: Select to activate the tunnel.

Add/Edit Tunnel – Routes

Adding routes allows you to configure what types of network traffic from the local host or hosts will be allowed through the tunnel.

Click **Add Route** to configure a new route. You will need to input the following information, defined by the remote network:

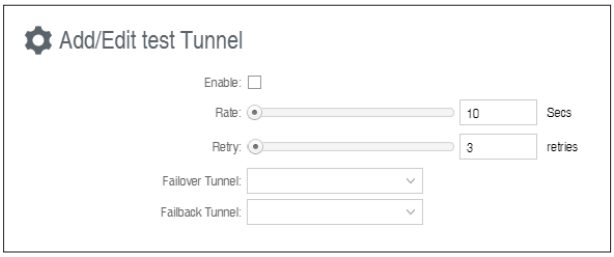
- **Network Address** – This is the network address that is the destination of the route. This should be set to the network address at the remote side of the tunnel.
- **Netmask** – This is the corresponding subnet mask of the network being defined (Default: 255.255.255.0).

You can set the tunnel to connect to a range of IP addresses or to a single IP address. For example, you could input **192.168.0.0** and **255.255.255.0** to connect your tunnel to all the addresses of the remote network in the **192.168.0.x** range. Alternatively, you could select a single address by inputting that address along with a Netmask of **255.255.255.255**.

Add/Edit Tunnel – Keep Alive

GRE keep-alive packets can be enabled to be sent through the tunnel in order to monitor the status of the tunnel and more accurately determine if the tunnel is alive or not.

GRE keep-alive packets may be sent from both sides of a tunnel, or from just one side.



©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Enabled: Select to enable GRE Keep Alive to continually send keep-alive packets to the remote peer.

Rate: Choose the length of time in seconds for each check (Default: 10 seconds. Range: 2 – 3600 seconds).

Retry: Select the number of attempts before the GRE tunnel is considered down or up (Default: 3. Range: 1 – 255).

Failover Tunnel and **Failback Tunnel**: Use these settings to create two tunnels – one as the primary tunnel and one as the backup tunnel. To configure tunnel failover/failback, complete the following steps:

1. Create two tunnels: one for primary and one for backup. Make sure both tunnels have **Keep Alive** enabled.
2. Choose one to be the primary tunnel. Open the editor for this tunnel and make sure **Tunnel Enabled** is selected. Then go to the **Keep Alive** page. Under **Failover Tunnel** select the other tunnel you have created.
3. Open the editor for the failover tunnel. Make sure **Tunnel Enabled** is *not* selected. On the **Keep Alive** page, set the **Failback Tunnel** to your primary tunnel.

NEMO

Network Mobility (NEMO) is an Internet standards track protocol defined in RFC 5177. The protocol allows session continuity for every node in a mobile network as the network moves.

NEMO requires a service provider, e.g. Verizon Wireless Private Network with DMNR (Dynamic Mobile Network Routing). Your NEMO service provider will define many of the settings for your NEMO configuration.

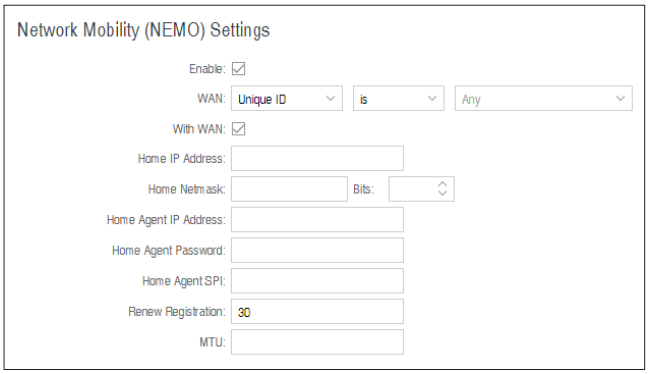
Once you have a NEMO service provider and a valid feature license, add networks to the **Networks Routed by NEMO** section by first clicking **Add**. In the popup window, input:

- **Network Address** - This is the network address that is the destination of the route. This should be set to the network address at the remote side of the tunnel.
- **Netmask** - This is the corresponding subnet mask of the network being defined (Default: 255.255.255.0).

The Network Address and Netmask, or subnet mask, together define a range of IP addresses that comprise the local network you want associated with the NEMO settings.

Network Mobility (NEMO) Settings

Enbable: Enable NEMO.



WAN: Select the WAN(s) to use for the NEMO connection. An expression such as "Unique ID is (any)" will allow NEMO to operate on any WAN, whereas "Type is LTE" will limit NEMO operation to the WAN(s) provided by any connected LTE device(s).

With WAN: Register the NEMO connection simultaneous with its specified WAN connection becoming available. If not checked, will only register the NEMO connection when needed.

Home IP Address and **Home Netmask** – These may be provided by your NEMO service provider. The IP address is a placeholder, "dummy" address; any IP address can be used (1.2.3.4 is common).

Home Agent IP Address, **Home Agent Password**, and **Home Agent SPI** – Your home agent will be defined by your NEMO service provider.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Renew Registration – The NEMO network regularly re-registers with the home agent (e.g., every 30 seconds). Specify the number of seconds between each check-in.

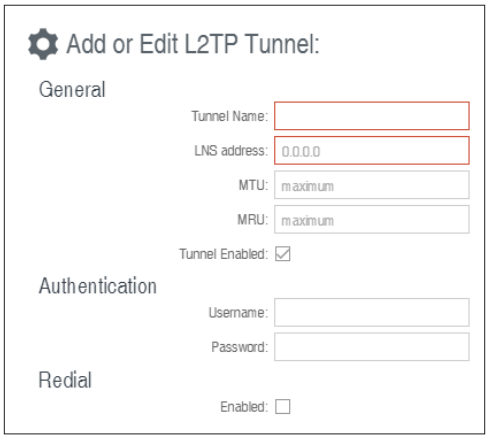
MTU – Override the maximum transmission unit (**MTU**) of the NEMO tunnel. The TCP **MSS** (maximum segment size) is automatically derived from the MTU. Leave blank to rely on **Path MTU Discovery**.

L2TP

Layer 2 Tunneling Protocol (**L2TP**) tunnels can be used to create a connection between two private networks.

Once you have a valid feature license, click **Add** to create a new L2TP tunnel. Click **Edit** to make changes to an existing tunnel.

Add/Edit Tunnel – General



- **Tunnel Name** – Enter a name to uniquely identify this tunnel
- **LNS address** – Enter the IP Address of the LNS (tunnel server) peer
- **MTU** – Set the maximum transmission unit (**MTU**) for the L2TP tunnel
- **MRU** – Set the maximum receive unit (MRU) to request from the tunnel peer. The MRU is very similar to the MTU: MTU is for packets sent and MRU is for packets received
- **Tunnel Enabled** – Click to enable/disable this tunnel. Default: Enabled.

Authentication

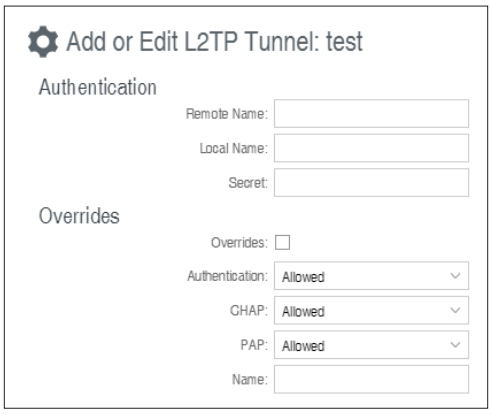
More authentication options and overrides are available in the next section.

- **Username** – Username for user-specific authorization. Leave blank to disable.
- **Password** – Shared secret (or password) used to authenticate the associated Local and Remote names.

Redial

- **Enabled** – When this is selected, the tunnel will attempt to reconnect if disconnected.

Add/Edit Tunnel – Authentication



- **Remote Name** – Authorization name specified by and to the remote system as its identity, sometimes a username or hostname. Leave blank to match any.
- **Local Name** – Authorization name specified by and to the remote system as the local system identity; sometimes a username or hostname. Leave blank to match any.
- **Secret** – Shared secret (or password) used to authenticate the associated Local and Remote names.

Overrides

Override Authentication methods/parameters. With methods set to Allow the two ends of the tunnel can negotiate a common scheme.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Sometimes this negotiation fails, or the implementation on one end is incompatible with the other. To solve those authentication issues, enable the overrides as needed.

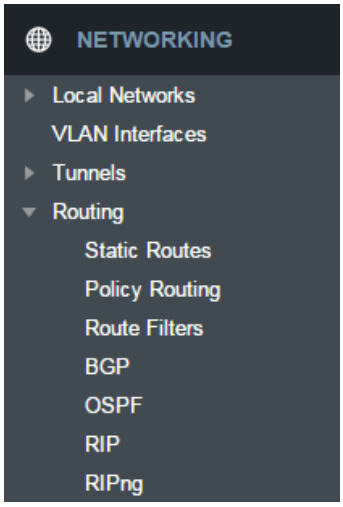
- **Authentication** – Username for user-specific authorization. Leave blank to disable.
- **CHAP** – Choose from Allowed, Refused, or Required.
- **PAP** – Choose from Allowed, Refused, or Required.
- **Name** – Override names used to authenticate the router. Leave empty to use the default.

Add/Edit Tunnel – Routes

Typically specific routes are unnecessary, but they can be added in this section if needed. You can add or remove routes to be used to funnel packets through the tunnel.

- **Network Address** – This is the network address that is the destination of the route. This should be set to the network address at the remote side of the tunnel.
- **Netmask** – This is the corresponding subnet mask of the network being defined.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com



ROUTING

STATIC ROUTES

Add a new static route to the IP routing table or edit/remove an existing route.

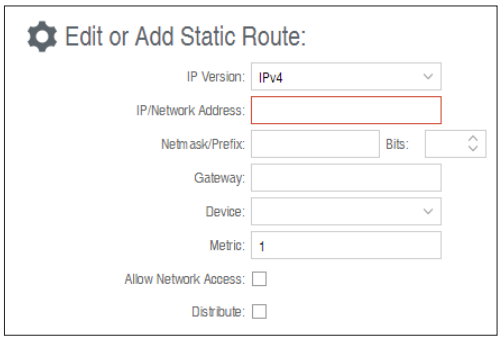
Static routes are used in networks with more than one layer, such as when there is a network within a network so that packet destinations are hidden behind an additional router. Adding a static route is a way of telling the router about an additional step that packets will need to take to reach their destination.

Click **Add** to create a new static route.

IP Version: Select IPv4 or IPv6. Depending on your selection, you have different options for defining the address range.

IP/Network Address or **IPv6 Address**: The IP address of the target network or host. The IPv6 address field includes **CIDR notation** to declare a range of addresses.

Netmask/Prefix: The Netmask, along with the IPv4 address, defines the network the computer belongs to and which other IP addresses the computer can see in the same LAN. An IP address of 192.168.0.1 along with a Netmask of 255.255.255.0 defines a network with 256 available IP addresses from 192.168.0.0 to 192.168.0.255.



Gateway or **IPv6 Gateway**: Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: **LAN** or **WAN**.

Device: Select the network interface from the dropdown menu (e.g. ethernet-wan). You can use this instead of defining the IP address, especially in cases when the IP address is changing.

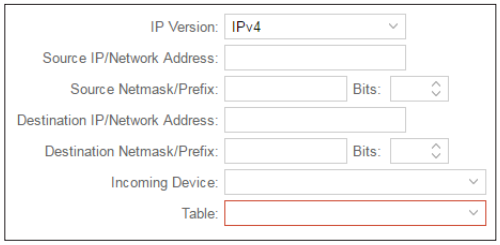
Metric: Set the numerical priority of the route. Lower numbers have higher priority.

Allow Network Access: (Default: Deselected.) Some static routes will need an IP Filter Rule via the Firewall to allow packets through the route without being blocked. Selecting this option automatically creates this IP Filter Rule. If the **IP/Network Address** falls outside the LAN IP range, you probably need to select this option.

Distribute: Allow this static route to be distributed via a routing protocol (BGP, OSPF, RIP, RIPng).

POLICY ROUTING

Policy routing allows for the addition of routes which are only evaluated when a certain set of conditions match. The evaluation occurs before the main system routes and can override the primary route table. If no policy route is matched, the lookup will fall back on the primary route table instead.

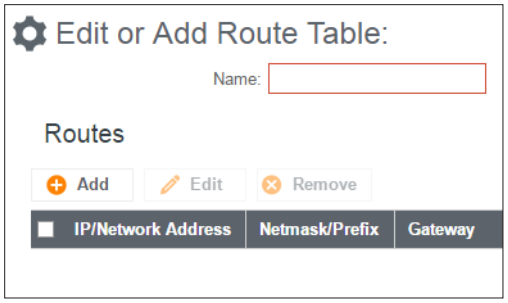


Route Policies: Route Policies define a policy to route table mapping. Any traffic matched by the policy will be routed according to the specified route table. If no policy or no route is matched, the lookup will use the primary route table instead. To add a route policy, click **Add**.

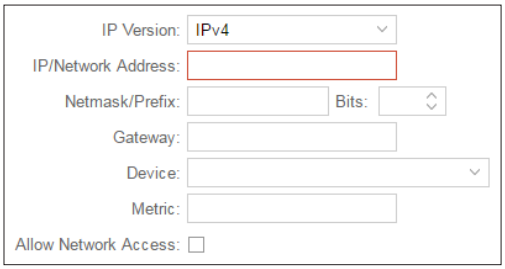
- **IP Version:** Select the IP protocol version.
- **Source IP/Network Address**

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- **Source Netmask/Prefix**
- **Destination IP/Network Address**
- **Destination Netmask/Prefix**
- **Incoming Device:** Select the incoming device upon which this policy will match. (optional)
- **Table:** Select the route table to use for routing when this policy is matched.



Route Tables: Static route tables to be used in policy route lookups. In order for route tables defined here to take effect, a corresponding Route Policy must be created. Note that route tables defined here are not available for use in dynamic routing protocols. To add a route, click **Add**.



- **IP Version:** Select the IP protocol version.
- **IP/Network Address**
- **Netmask/Prefix**
- **Gateway**
- **Device:** Select the interface or enter null0 to install a black hole route.
- **Metric:** Set the route metric.
- **Allow Network Access:** Some static routes will need an IP Filter Rule added to allow packets to route without being blocked by the firewall. Clicking the check box will automatically add this rule for you.

ROUTE FILTERS

Common route filters may be used by any of the routing protocols. When shown in selection UI, filter names are prepended with a label to identify the type, i.e. al:AccessListName, pl:PrefixListName, and rm:RouteMapName. Filter names must be unique across all filters, common and protocol-specific.

Route filter entries are processed in the order in which they appear in the grid. A match will apply the action (permit or deny) specified for the entry and processing will stop. If a filter is referenced and no match is found, the route is denied.

Access List: Allows packet filtering by IP address.

Prefix List: Works the same as an access list with the addition of filtering by prefix length. If the IP Network matches, the filter will match if the prefix length is less than or equal to the 'le' value, or greater than or equal to the 'ge' value. 'le' and 'ge' are optional, if both are omitted the prefix list acts as an access list.

Route Map: Provides a richer set of match conditions for packet filtering than access or prefix lists, and allows policy to be applied to a route via set actions.

- **Description:** Displayed to help identify the route map.
- **Permit:** Checking Permit will carry out the Set Actions if the Match Conditions are met, and permit the route. Clearing Permit will deny the route if the Match Conditions are met.
- **Match Conditions:** A set of conditions that define a match.
- **Set Actions:** A set of actions that are triggered by a match.

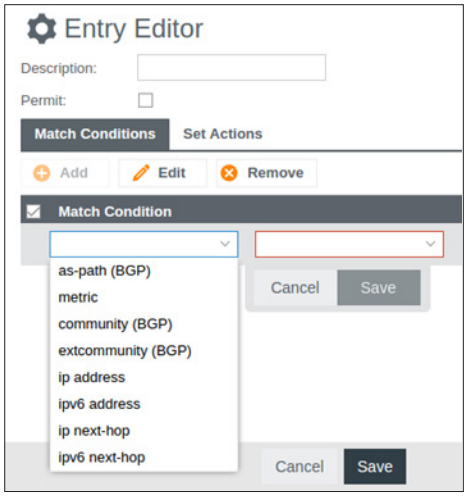
Certain match conditions and set actions are protocol-specific. Referencing a protocol-specific route map from an incompatible protocol will cause errors during operation that prevent the routing protocol from starting.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- **OSPF-specific:** metric-type.
- **BGP-specific:** as-path, weight, comm-list, local-preference, community, ext community.

A community is identified by a 32-bit value (e.g. 1234567890) usually expressed as two 16-bit values separated by a colon (e.g. 18838:722). A received or well-known community can be referenced by its number (or number pair), while defining a community list allows naming and refering to it by name.

Note certain well-known communities can be used by name without definition: **no-advertise** (never advertise these routes), **no-export** (don't advertise beyond confederation boundary), **local-AS** (don't advertise to external peers), **internet** (advertise to everyone), and **none** (used to clear any community associated with a route).

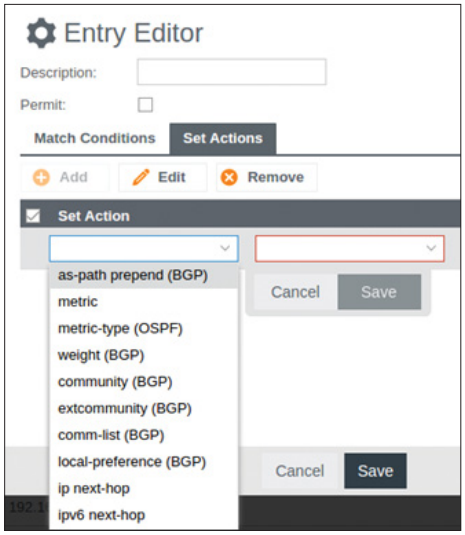


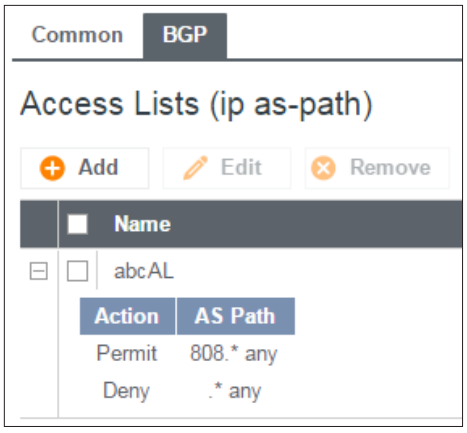
BGP route filters are only used by the BGP protocol. Access lists are prepended with 'fl:' when shown in selection UI. Community lists are prepended with 'cl:'. Filter names must be unique across all filters, common and protocol-specific.

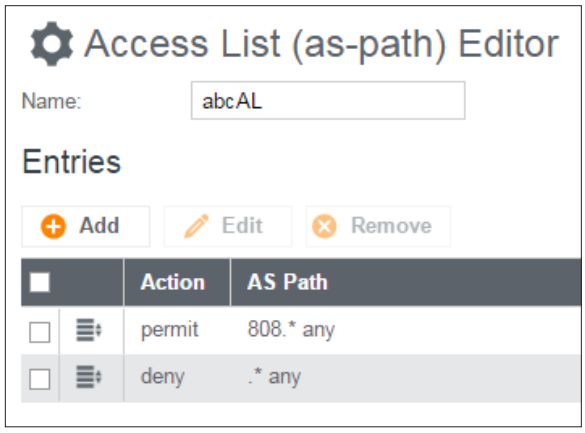
Route filter entries are processed in the order in which they appear in the grid. A match will apply the action (permit or deny) specified for the entry and processing will stop. If a filter is referenced and no match is found, the route is denied.

Access List: The ip as-path access-list allows filtering by BGP as-path. The as-path value can be specified as a regular expression (regex).

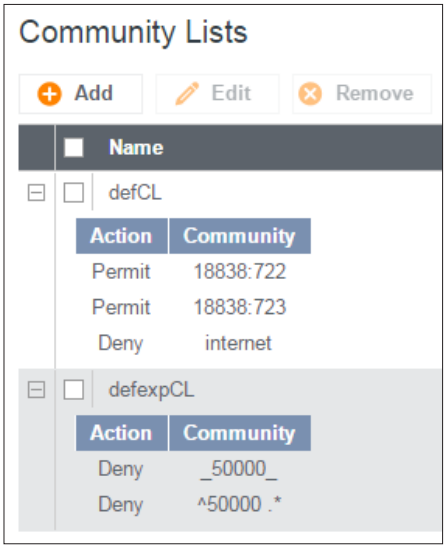
Community List: Allows filtering by community. In essence a community is a label which is attached to routes learned from that community. Then that community or label can be used to select which policy(s) should be applied to those routes.

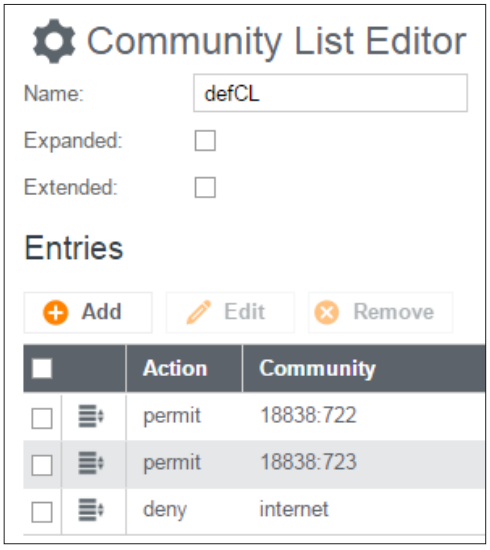






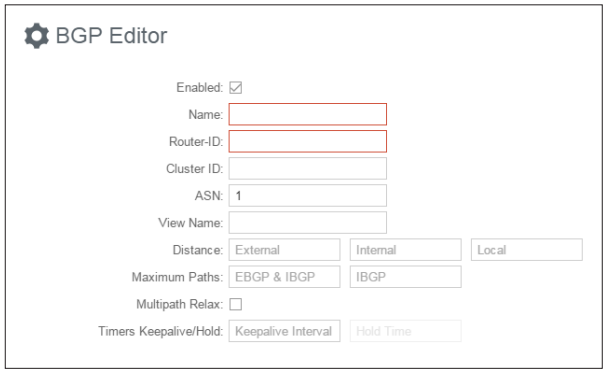
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com





BGP

The latest version of BGP (Border Gateway Protocol) is version 4. BGP-4 is one of the Exterior Gateway Protocols and de facto standard of Inter Domain routing protocol. BGP-4 is described in RFC1771, A Border Gateway Protocol 4 (BGP-4). BGP is a distance vector routing protocol, and the AS-Path framework provides distance vector metric and loop detection to BGP RFC1930.



BGP Editor

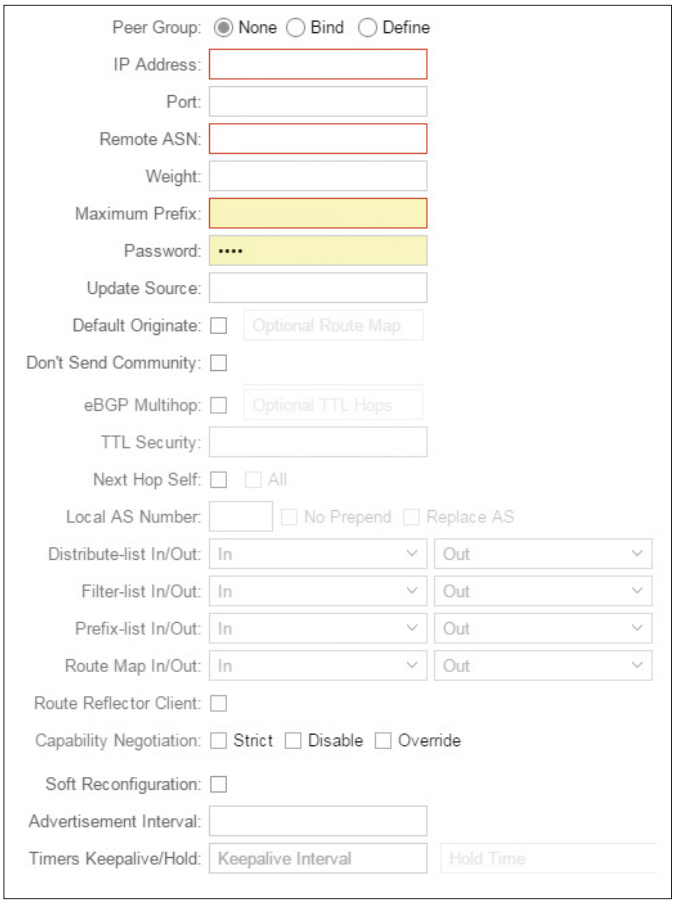
- **Enabled:** Click to enable/disable the policy. (Default: enabled).
- **Name**: Unique name of the policy.
- **Router-ID**: This sets the router-ID of the BGP process. The router-ID may be an IP address of the router, but need not be – it can be any arbitrary 32-bit number. However it *MUST* be unique within the entire BGP domain to the BGP speaker: bad things will happen if multiple BGP speakers are configured with the same router-ID.
- **Cluster ID:** Specify the cluster ID, used if the BGP cluster has more than one route reflector.
- **ASN**: The AS (Autonomous System) number is one of the essential elements of BGP.
- **View Name:** Specify a view to exchange BGP routing information without adding to the kernel routing table.
- **Distance:** The Administrative Distance can be specified for each of External (EBGP), Internal (IBGP) and Local routes, respectively. Defaults of 20, 200 and 200 will apply for any unspecified distance if any distance is specified.
- **Maximum Paths:** Maximum Paths can be set greater than 1 to allow multipath routing. This setting limits the number of paths; resources will be allocated to the limit specified whether or not all paths are used. The first field sets a limit for both EBGP and IBGP. If desired, a different limit can be applied just to IBGP using the second field.
- **Multipath Relax:** Select “relax” to allow multi-path routing to different ASNs.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- **Timers Keepalive/Hold**: Keepalive interval is the time between keepalive messages sent to peers. Hold time is the timeout after the last keepalive message until the peer is declared dead. The Keepalive interval must be set in order to set the Hold time. All times are in seconds from 1 to 65535. Set to 0 or empty to disable (default).

Networks Associated with ASN or **IPv6 Networks Associated with ASN**: To configure a BGP router, you need an AS number. An AS number is an identification of autonomous system. BGP protocol uses the AS number for detecting whether the BGP connection is internal one or external one. Use the IPv4 address and netmask or IPv6 address with a **CIDR notation** prefix length to define the address range.

Neighbor Options or **IPv6 Neighbor Options**: Creates a new neighbor identified by remote ASN and IP address.



- **Peer Group:** Optionally specify a peer group for this neighbor. You can **Bind** to an existing peer group or **Define** a new one. A neighbor will inherit the properties from the peer group to which it is bound. Properties specified in a neighbor will override inherited properties.
- **IP Address:** The IP address of the neighbor. Not specified if this is a peer group definition.
- **Port:** Specify port.
- **Remote ASN:** Enter the ASN of the remote AS. The AS (Autonomous System) number is one of the essential elements of BGP. BGP is a distance vector routing protocol, and the AS-Path framework provides distance vector metric and loop detection to BGP. RFC1930.
- **Weight:** Assign a weight to a neighbor connection.
- **Maximum Prefix:** Specify the maximum number of prefixes that a BGP routing process will accept from the specified peer.
- **Password:** Enable message digest5 (MD5) authentication on a TCP connection between BGP peers. The same password must be used on both peers.
- **Update Source:** Specify the IPv4 source address or interface name to use for the BGP session to this neighbor.
- **Default Originate:** Allow the local router to send the default route (0.0.0.0) to a neighbor for use as a default route. Optionally, a route map can be specified to conditionally inject the default route.
- **Don't Send Community:** Unless this option is selected, any defined communities attributes will be sent to the BGP neighbor.
- **eBGP Multihop:** Accept and attempt BGP connections to external peers residing on networks that are not directly connected. Mutually exclusive with TTL Security. Optionally specify Time To Live from 1 to 255 hops.
- **TTL Security:** Specify the number of hops to reach eBGP neighbors. Mutually exclusive with eBGP Multihop.
- **Next Hop Self:** Configure the router as the next hop for a BGP-speaking neighbor or peer group if it is learned via eBGP. Select **All** to also apply this setting to routes learned via iBGP.
- **Local AS Number:** Enter the AS Number used locally as this neighbor's prefix. It is prepended to the received AS_PATH when receiving routing updates from the peer, and prepended to the outgoing AS_PATH when transmitting local routes to the peer. Check **No Prepend** to not prepend the local AS Number to either

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

the received or outgoing AS_PATH. Check **Replace AS** to prepend the local AS Number to just the outgoing AS_PATH.

- **Distribute-list In/Out:** Specify a distribute-list for the peer in either or both directions. Lists are chosen from the collection of access lists and prefix lists defined in Route Filters, Common tab. Access list and prefix list names are prepended with 'al' and 'pl', respectively.
- **Filter-list In/Out:** Filter this neighbor's incoming and/or outgoing advertisements according to the specified as-path access list(s). Lists are chosen from the collection of as-path access lists defined in Route Filters, BGP tab.
- **Prefix-list In/Out:** Filter this neighbor's incoming and/or outgoing advertisements according to the specified prefix list(s). Lists are chosen from the collection of prefix lists defined in Route Filters, Common tab.
- **Route Map In/Out:** Apply a route map to incoming and/or outgoing routes. Maps are chosen from the collection of route maps defined in Route Filters, Common tab.
- **Route Reflector Client:** Configures the router as a BGP route reflector and configures the neighbor as its client.
- **Capability Negotiation:** Configure capability negotiation with the remote peer. Select **Strict** to completely match capabilities. Select **Disable** to suppress sending a negotiation message to peers that are not configured as IPv4 unicast. Select **Override** to ignore the remote peer's capability value and use the local value instead.
- **Soft Reconfiguration:** Configure the router to store updates.
- **Advertisement Interval:** Configure the interval for BGP routing updates, in seconds from 0 to 600.
- **Timers Keepalive/Hold: Keepalive interval** is the time between keepalive messages sent to peers. **Hold time** is the timeout after the last keepalive message until the peer is declared dead. The **Keepalive interval** must be set in order to set the **Hold time**. All times are in seconds from 1 to 65535. Set to 0 or empty to disable (default).

Redistribute Routes: Redistribute routes of the specified protocol or kind into BGP, with the metric type and metric set if specified, filtering the routes using the given route map if specified. Redistributed routes may also be filtered with distribute lists.

- **Type**: The type is the source of the route. Select from: Main, Connected, Static, RIP, and OSPF.
- **Metric**: Numerical priority of the route.
- **Route Map**: Route maps provide a means to filter and/or apply actions to routes, allowing policies to be applied to routes.

OSPF

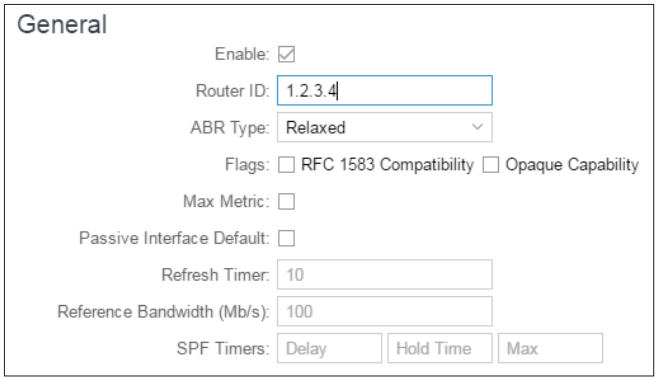
OSPF (Open Shortest Path First) version 2 is a routing protocol described in RFC2328, OSPF Version 2. OSPF is an IGP (Interior Gateway Protocol). Compared with RIP, OSPF can provide more scalable network support and faster convergence times. OSPF is widely used in large networks such as ISP (Internet Service Provider) backbone and enterprise networks. Click **Add** to add an OSPF router.

General

- **Enable**: Enable and disable the routing protocol policy.
- **Router ID**: OSPF routers are identified by a unique ID which must be a dotted quad (like an IP address). This ID MUST be unique within the entire OSPF domain - errors will happen if multiple OSPF speakers are configured with the same router-ID.
- **ABR Type:** The OSPF standard does not allow an ABR to consider routes through connected non-backbone areas. **Relaxed** (default) relaxes this restriction and will consider routes through non-backbone areas if the

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

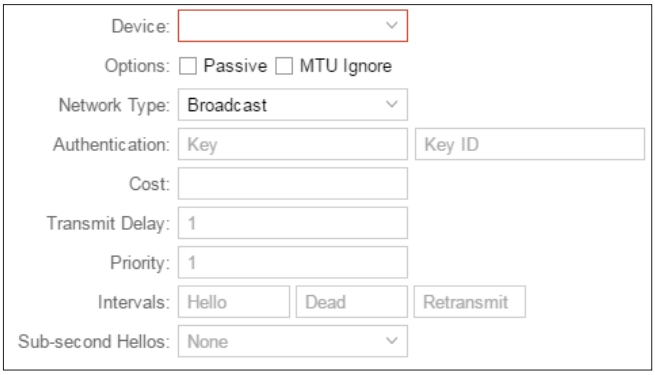
backbone area is down. **Standard** respects the OSPF standard regardless if the backbone area is down. **Shortcut** will always route through the best path even if it does not go through the backbone area. When this is set, shortcut can be enabled/disabled on a per area basis.



- **Flags**: RFC 1583 Compatibility uses the predecessor standard RFC 1583 path preference algorithm. This typically is NOT set. Opaque capability enables forwarding Opaque LSA extensions described in RFC 5250.
- **Max Metric:** Set this router to broadcast max (infinite-distance) metric. Essentially broadcasting that this router is unreachable.
- **Passive Interface Default:** By default, any interface that controls a defined OSPF network will send link-state advertisements. Set Passive Interface Default to allow only interfaces configured under Interfaces to send link-state advertisements.
- **Refresh Timer:** Sets the OSPF LSA refresh timer. Default is 10 seconds.
- **Reference Bandwith (Mb/s):** Sets the reference bandwidth for cost calculations. Link cost will automatically scale in reference to this bandwidth unless explicitly overridden. The default is 100 Mb/s equal to cost of 1. Note: this setting MUST be consistent across routers in the OSPF domain.
- **SPF Timers:** Sets the shortest path first algorithm adaptive timers in milliseconds. Modifying these values allows you to manage CPU usage when calculating SPF. Delay sets the initial delay. SPF calculations will always be performed at least this many milliseconds apart. Consecutive SPF calculations will always be separated by at least the Hold Time up to the Max Hold Time increasing by Max Hold Time for each consecutive calculation.

Interfaces

- **Device**: Select device interface.
- **Options**: Set interface options. **Passive** means no Hellos will be transmitted out this interface. **MTU Ignore** disables MTU mismatch detection.
- **Network Type**: Set the network type for this interface.
- **Authentication:** Set OSPF interface authentication. **Key** sets the OSPF authentication key to a simple password. After setting authentication key, all OSPF packets are authenticated. The authentication key has a maximum length of eight characters if using plain text authentication and sixteen characters if using message-digest authentication. **Key ID** enables message-digest authentication. Leave this blank to enable plain text authentication. The Key ID identifies the secret key used to create the message digest. This ID is part of the protocol and must be consistent across routers on a link.



- **Cost:** OSPF metric for this interface.
- **Transmit Delay:** Link state transmit delay.
- **Priority:** The router with the highest priority will be more eligible to become Designated Router. Setting this to 0 disables this router from participating in DR elections.
- **Intervals:** Set hello intervals. **Hello** sets the number of seconds for the Hello Interval timer value. Setting this value, Hello packets will be sent every timer value seconds. This value must be the same for all routers

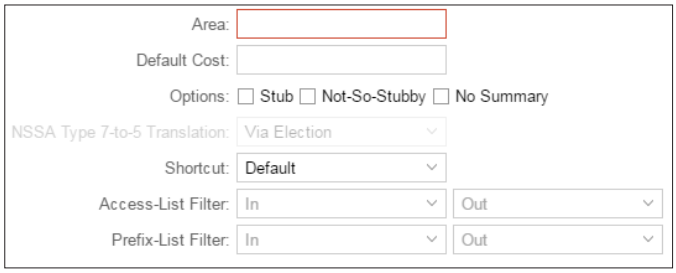
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

in the area. The default value is 10 seconds. **Dead** sets the number of seconds for the Router Dead Interval timer value used for Wait Timer and Inactivity Timer. This value must be the same for all routers attached an area. The default value is 40 seconds. **Retransmit** sets the number of seconds between retransmitting lost link state advertisements.

- **Sub-second Hellos:** Enable sub-second Hellos and set the number of Hellos per second. When set, Dead Interval is set to one second.

Areas

- **Area:** Areas are identified by a unique ID which may be a 32-bit unsigned integer or a dotted quad (like an IP address).
- **Default Cost:** Set the cost of default-summary LSAs announced to stubby areas.
- **Options:** Set options for this area. **Stub** indicates that this area is a stub and no area router will propagate routes external to OSPF and AS-External LSAs (Type-5s) or ASBR-Summary LSAs (Type-4) will be propagated into the area. Only Network-Summary (Type-3) and default-route summary advertisements will be propagated. **Not-So-Stubby** indicates this area is Not-So-Stubby or NSSA. This is similar to a stubby area except external routes are propagated as Type-7 LSAs. NSSA Type-7 NSSAs can optionally be configured to be translated to Type-5 LSAs with the **NSSA Translate** option set. **No Summary** Prevents ABR from injecting inter-area summaries into the specified stub or Not-So-Stubby area. Default routes will be injected as a type 3 summary LSA.



- **NSSA Type 7-to-5 Translation:** Method of translating Type-7 LSAs to Type-5 when propagating external routes. **Via Election** indicates this router is an NSSA Border Router but other border routers exist in the topology. It will perform Type-7 to Type-5 translation unless another border router has Always set or is set to Via Election and has a higher router-id. **Always** indicates this is an NSSA Border Router and must always perform Type-7 tp Type-5 LSA translations. **Never** indicates that this router must never perform Type-7 to Type-5 LSA translations.
- **Shortcut:** **Enable** or **disable** shortcuts through non-backbone areas. **Default** will shortcut only if the backbone link is down. Requires that **ABR Type** be set to **Shortcut**.
- **Access-List Filter:** Filter Type-3 summary LSAs to/from area using access lists. This is only applicable on ABR.
- **Prefix-List Filter:** Filter Type-3 summary LSAs to/from area using prefix lists. This is only applicable on ABR.

Redistribute

- **Default Originate:** Enable broadcasting default route. **Always** will cause the default route (0.0.0.0/0) to be broadcast even if it is not in the routing table. **Metric** specifies the metric of the default route. **Metric Type** is the OSPF metric type (default Type-2). **Route Map** specifies an optional route map to filter routes.
- **Default Metric:** Specify the default metric for routes redistributed to OSPF. This can be overridden under the **Redistribute** configuration.
- **Default Distance:** Sets the default administrative distance for **intra-area**, **inter-area** and **external** routes. Specific distances can be set under **Distances**. The default is 110.

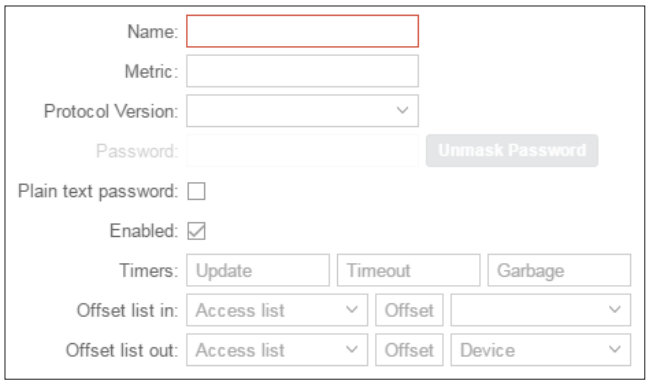
- **Distances:** Specify administrative distances for **intra-area**, **inter-area**, or **external** routes. This overrides the value set in **Default Distance**.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

RIP

RIP (Routing Information Protocol) is a widely deployed interior gateway protocol. RIP is a distance-vector protocol based on the Bellman-Ford algorithms. As a distance-vector protocol, RIP sends updates from one router to its neighbors periodically, allowing the convergence to a known topology. In each update, the distance to any given network will be broadcast to its neighboring router. The router supports RIP version 2 as described in RFC2453 and RIP version 1 as described in RFC1058.

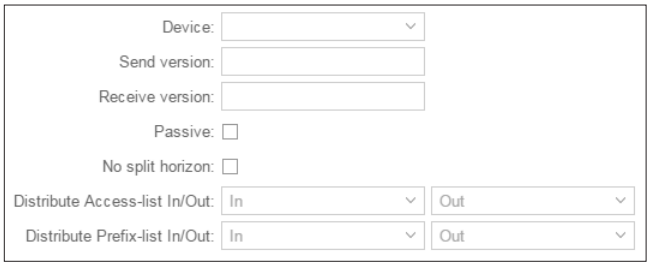
RIP Editor



- **Name**: Unique name of the policy.
- **Metric**: RIP metric is a value for distance for the network. Usually RIP increments the metric when the network information is received. The metric for redistributed routes is set to 1.
- **Protocol Version**: RIP can be configured to send either version 1 or version 2 packets. The default is to send RIPv2 while accepting both RIPv1 and RIPv2 (and replying with packets of the appropriate version for REQUESTS / triggered updates).
- **Password**: RIPv2 allows packets to be authenticated via either an insecure plain text password, included with the packet, or a more secure MD5 based HMAC (keyed-Hashing for Message AuthentiCation). RIPv1 cannot be authenticated at all, so when authentication is configured RIP will discard routing updates received via RIPv1 packets.
- **Plain text password**: Select to use a plain text password instead of an MD5 HMAC. WARNING: A plain text password is insecure.
- **Enabled:** Click to enable/disable the policy. (Default: enabled.)
- **Timers: Update** specifies the period at which the routing table is sent to all neighbors. Default is 30 seconds. **Timeout** specifies the length of time that the route is valid. Default is 180 seconds. **Garbage** specifies the garbage collection timer that triggers removal of the route from the routing table. Default is 120 seconds.
- **Offset list in:** Offset-list adds the specified offset to the incoming and outgoing metric for routes matched by the specified access-list. If the offset is 0, no action is taken.
- **Offset list out:** Offset-list adds the specified offset to the incoming and outgoing metric for routes matched by the specified access-list. If the offset is 0, no action is taken.

Networks: Set the RIP-enabled interfaces by network. RIP is enabled on the interfaces that have addresses within the network range.

Interfaces: Enable RIP on a specific interface. Useful if the interface's IP addresses are dynamic.



- **Device:** Select network interface device.
- **Send version:** Select the RIP version that will be sent on this interface, overriding the global setting. Version can be 1 or 2, or 0 to select both.
- **Receive version:** Select the RIP version that will be accepted on this interface, overriding the global setting. Version can be 1 or 2, or 0 to select both.
- **Passive:** Select passive mode for the interface. In passive mode, RIP routing updates are accepted by, but not sent out of, the interface.
- **No split horizon:** Disable the split horizon mechanism. Enabling prevents RIP from advertising routes over the interface on which they were learned.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- **Distribute Access-list In/Out:** Specify access-lists that filter the incoming and outgoing distribution of RIP routes.
- **Distribute Prefix-list In/Out:** Specify prefix-lists that filter the incoming and outgoing distribution of RIP routes.

Neighbors: When a neighbor doesn't understand multicast, this command is used to specify neighbors. In some cases, not all routers will be able to understand multicasting, where packets are sent to a network or a group of addresses. In a situation where a neighbor cannot process multicast packets, it is necessary to establish a direct link between routers. The neighbor command allows the network administrator to specify a router as a RIP neighbor. The no neighbor a.b.c.d command will disable the RIP neighbor. Assign a neighbor by inputting an IP address.

Redistribute Routes: Redistribute routes of the specified protocol or kind into RIP, with the metric type and metric set (if specified), filtering the routes using the given route map (if specified). Redistributed routes may also be filtered with distribute lists.

- **Type**: The type is the source of the route. Select from: Main, Connected, Static, OSPF, BGP.
- **Metric**: RIP metric is a value for distance for the network. Usually RIP increments the metric when the network information is received. The metric for redistributed routes is set to 1.
- **Route Map**: Route maps provide a means to filter and/or apply actions to routes, allowing policies to be applied to routes.

RIPng

RIPng (RIP next generation) extends RIPv2 to support IPv6. See **RIPng on Wikipedia** and **RFC 2080** for details.

RIPng Editor

- **Name**: Unique name of the policy.
- **Metric**: RIPng metric is a value for distance for the network. Usually the RIP service increments the metric when the network information is received. The metric for redistributed routes is set to 1.
- **Enabled**: Click to enable/disable the policy. (Default: enabled.)

Networks: Set the RIPng-enabled interfaces by network using IPv6 addresses. RIPng is enabled on the interfaces that have addresses within the network range.

Routes: Set RIPng static routing announcement of specified network address.

Redistribute Routes: Redistribute routes of the specified protocol or kind into RIPng, with the metric type and metric set if specified, filtering the routes using the given route-map if specified.

- **Type**: The type is the source of the route. Select from: Main, Connected, Static, OSPF, BGP.
- **Metric**: RIPng metric is a value for distance for the network. Usually the RIP service increments the metric when the network information is received. The metric for redistributed routes is set to 1.
- **Route Map**: Route maps provide a means to filter and/or apply actions to routes, allowing policies to be applied to routes.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

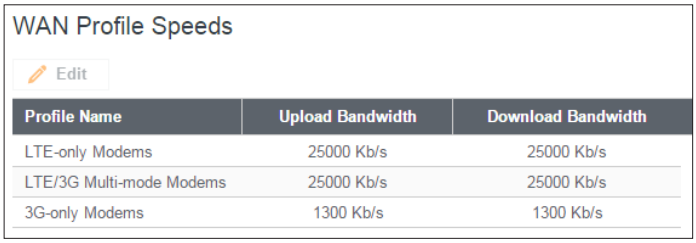
QOS

When QoS (Quality of Service, also known as "Traffic Shaping") is enabled, the router will control the flow of Internet traffic according to the user-defined rules. In other words, Traffic Shaping improves performance by allowing the user to prioritize applications.

Enable QoS: Click on this box to open options for controlling Internet traffic. You can assign maximum Upload Speed and Download Speed values and define your own Traffic Shaping rules.

WAN Profile Speeds

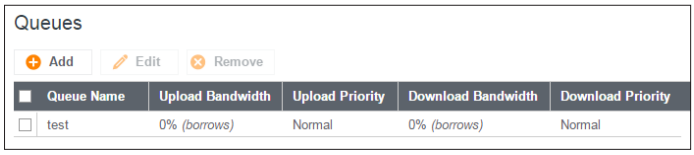
Upload Speed and Download Speed: Setting the Upload Speed and Download Speed is required to control traffic flow accurately. Adjust the sliding bar to restrict the maximum upload and/or download speed for the Internet source(s) you are using. For example, you might restrict the upload speed to prioritize available bandwidth for download or to reduce overall bandwidth use in order to lower costs. It is recommended that you experiment with different values for your particular Internet connection for best results.



NOTE: Upload speed is the speed at which data can be transferred to your ISP. Download speed is the speed at which data can be transferred to you from your ISP. You can test your connection speeds with a service such as speedtest.net.

Queues

Queues and rules work in conjunction to prioritize bandwidth for the most critical operations. Multiple rules can be associated with one queue. Use rules to associate your more critical operations with queues that have higher bandwidth settings. For example, you might have two queues, one for "critical" and one for "secondary" with critical having most of the bandwidth percentage. Use rules to associate your most important bandwidth needs (POS system, VoIP, etc.) with the critical queue. Restrict the bandwidth available for less important functions with the secondary queue.



Assign percentages of both upload and download bandwidth to each queue. If you assign 80% download bandwidth to the first queue, the next queue will be forced to be 20% or less.

Click **Add** to create a new Traffic Shaping/QoS queue.

Queue Name: Choose a name that is meaningful to you.

DSCP (DiffServ) Tag: Differentiated Services Code Point (DSCP) is the successor to TOS (Type of Service). Use this field to 'tag' the traffic by putting the value in the DSCP header of each IP packet that flows through this queue. Use the value of '0' to clear the existing DSCP value in the packet header.

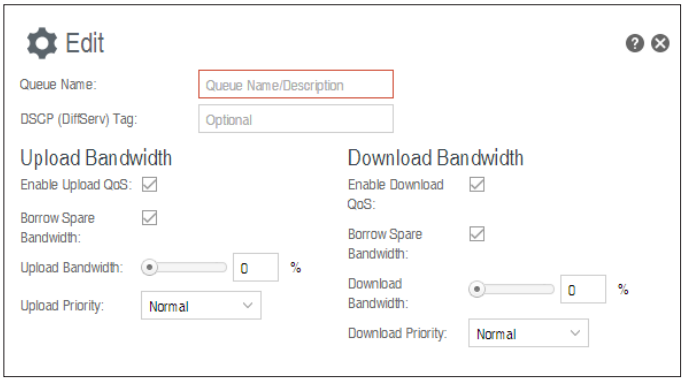
DSCP Tagging is sometimes used so that other networking equipment, upstream or post-NAT, can do traffic shaping based on the DSCP Tags as opposed to IP addresses or ports.

This setting is optional.

Upload Bandwidth

Enable Upload QoS: (Default: Enabled.) Deselect if you want your rule to apply to download traffic only. Leave this selected to include upload restrictions with this queue.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com



Borrow Spare Bandwidth: (Default: Enabled.) When this is enabled, the interfaces/protocols associated with this rule will borrow unused bandwidth from other rules. Disabling borrowing will restrict the traffic to the specified bandwidth. Higher priority queues will be offered excess bandwidth first.

Upload Bandwidth: This is the percentage of the connected WAN upload bandwidth that will be reserved for the specified traffic. The maximum value is adjusted to the remaining percentage after other rules receive their share.

Upload Priority: The priority value has two different effects on traffic. Higher priority traffic is handled before lower priority traffic, which can lead to shorter response times. Also, when spare bandwidth is available it is offered to higher priority queues first. Move the slider to select from the following options (Default: Normal):

- Lowest
- Lower
- Below Normal
- Normal
- Above Normal
- High
- Higher
- Highest

Click **Next** to continue to the next page.

Download Bandwidth

Enable Download QoS: (Default: Enabled.) Deselect if you want your rule to apply to upload traffic only. Leave this selected to include download restrictions with this queue.

Borrow Spare Bandwidth: (Default: Enabled.) When this is enabled, the interfaces/protocols associated with this rule will borrow unused bandwidth from other rules. Disabling borrowing will restrict the traffic to the specified bandwidth. Higher priority queues will be offered excess bandwidth first.

Download Bandwidth: This is the percentage of the connected WAN upload bandwidth that will be reserved for the specified traffic. The maximum value is adjusted to the remaining percentage after other queues receive their share.

Download Priority: The priority value has two different effects on traffic. Higher priority traffic is handled before lower priority traffic, which can lead to shorter response times. Also, when spare bandwidth is available it is offered to higher priority queues first. Move the slider to select from the following options (Default: Normal):

- Lowest
- Lower
- Below Normal
- Normal
- Above Normal
- High
- Higher
- Highest

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Click **Finish** to save this queue.

Rules
A traffic shaping rule identifies a specific message flow and assigns that flow to one of the queues created above.

Click **Add** to create a new Traffic Shaping rule.

Traffic Shaping / QoS Rule Editor
The first page of the Traffic Shaping / QoS Rule Editor allows you enable/disable the rule, name the rule, specify a protocol for the rule, and select a queue to associate the rule with.

Rule Enabled: (Default: Enabled.) Deselect this to disable this rule. This can be useful for quickly changing configurations. If both upload QoS and download QoS are disabled then the rule will disable automatically.

Rule Name: Create a name for the rule that is meaningful to you.

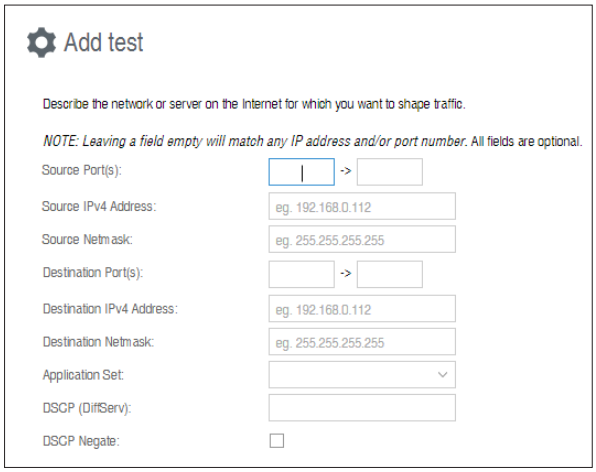
Protocol: The protocol used by the messages: TCP/UDP, TCP, UDP, or ICMP. Select "Any" if your rule does not control a specific type of message that uses a specific protocol.

Queue Name: Select a queue to associate this rule with.

Click **Next** to continue to the next page.

Use ports and/or IP addresses to define the type(s) of traffic attached to this rule. Leaving any field blank will match all values; all fields are optional.

Source Port(s) and/or Destination Port(s): Enter a port number between 1 and 65535. To enter a single port number, input the number into the left box. To enter a range of ports, fill in both boxes separated by the colon. For example "80:90" would represent all ports between 80 and 90 including 80 and 90 themselves.



Source IP Address, Source Netmask, Destination IP Address, and Destination Netmask: Specify an IP address or range of IP addresses by combining an IP address with a netmask for either "source" or "destination" (or both). Source vs. destination is defined by traffic flow. Leave these blank to include all IP addresses (such as if your rule is defined by a particular port instead).

EXAMPLE: If you want to associate this rule with your guest LAN, you could input the IP address and netmask for the guest LAN here (leaving the last slot "0" to allow for any user attached to the guest network):

- Source IP Address: 192.168.10.0
- Source Netmask: 255.255.255.0

Application Set: Application sets can be defined in the Application Sets tab of the Firewall Configuration page. The application identification might not take place until multiple packets have already bypassed a rule. Application sets require an active license to exist on the device for them to function.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

DSCP (DiffServ): Differentiated Services Code Point (DSCP) is the successor to TOS (Type of Service). Use this field to select traffic based on the DSCP header in each IP packet. This field is sometimes set by latency sensitive equipment such as VoIP phones. This setting is optional.

DSCP Negate: When checked this rule will match on any packet that does not match the DSCP field.

Click **Finish** to save this rule.

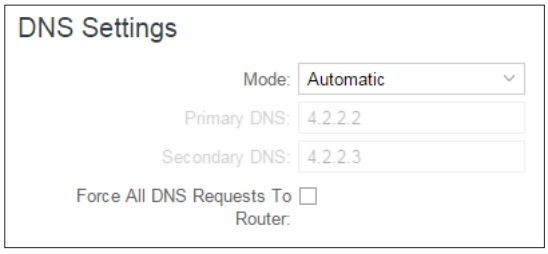
DNS SERVERS

DNS, or Domain Name System, is a naming system that translates between domain names (www.cradlepoint.com, for example) and Internet IP addresses (206.207.82.197). A DNS server acts as an Internet phone book, translating between names that make sense to people and the more complex numerical identifiers. The DNS page for the device has these distinct functions:

- **DNS Settings**: By default your router is set to automatically acquire DNS servers through your Internet provider (Automatic). DNS Settings allows you to specify DNS servers of your choosing instead (Static).
- **Split DNS**: Enable or disable the redirecting of specified domains to alternate DNS servers.
- **Dynamic DNS Configuration**: Allows you to host a server (Web, FTP, etc.) using a domain name that you have purchased (www.example.com) with your dynamically assigned IP address.
- **Known Hosts Configuration**: Allows you to map a name (printer, scanner, laptop, etc.) to an IP address of a device on the network.

DNS Settings

You have the option to choose specific DNS servers for your network instead of using the DNS servers assigned by your Internet provider. The default DNS servers are usually adequate. You may want to assign DNS servers if the default DNS servers are performing poorly, if you want WiFi clients to access DNS servers that you use for customized addressing, or if you have a local DNS server on your network.



Mode: Automatic or Static (default: Automatic). Switching to "Static" enables you to set specific DNS servers in the **Primary DNS** and **Secondary DNS** fields.

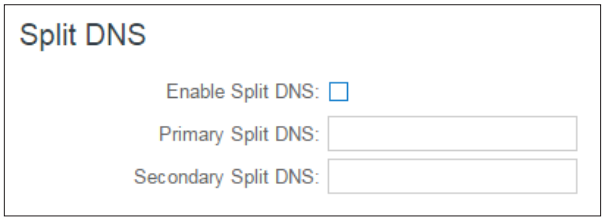
Primary DNS and **Secondary DNS**: If you choose to specify your DNS servers, then enter the IP addresses of the servers you want as your primary and secondary DNS servers in these fields. The DNS server settings will be pre-populated with public DNS server IP addresses. You can override the IP address with any other DNS server IP address of your choice. For example, Google Public DNS servers have the IP addresses 8.8.8.8 and 8.8.4.4 while 4.2.2.2 and 4.2.2.3 are servers from Level 3 Communications.

Force All DNS Requests To Router: Enabling this will redirect all DNS requests from LAN clients to the router's DNS server. This will allow the router even more control over IP addresses even when clients have their own DNS servers statically set.

Split DNS

Split DNS allows you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

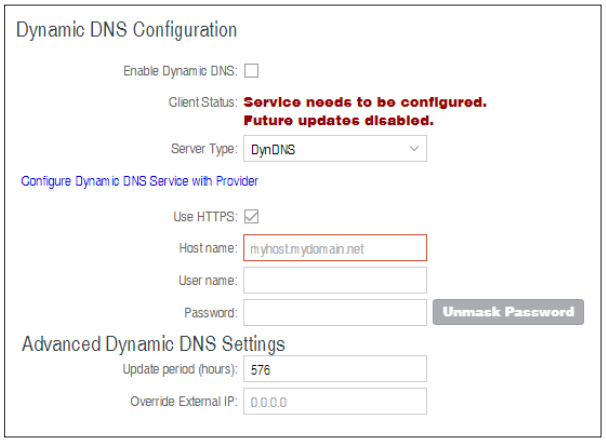


Primary Split DNS and **Secondary Split DNS**: If you choose to specify your DNS servers, then enter the IP addresses of the servers you want as your primary and secondary DNS servers in these fields. The Secondary DNS is optional.

Domain: Click **Add** to add desired domain for Split DNS.

Dynamic DNS Configuration

The Dynamic DNS feature allows you to host a server (Web, FTP, etc.) using a domain name that you have purchased (www.yourname.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, you can enter your host name to connect to your server, no matter what your IP address is.



- **Enable Dynamic DNS**: Enable this option only if you have purchased your own domain name and registered with a Dynamic DNS service provider.
- **Server Type**. Select a dynamic DNS service provider from the dropdown list:
  - **DynDNS**
  - **DNS-O-Matic**
  - **ChangeIP**
  - **NO-IP**
  - **Custom Server (DynDNS clone)**
- **Custom Server Address**. Only available if you select Custom Server from the Server Address dropdown list. Enter your custom DynDNS clone server address here. For example: www.mydyndns.org.
- **Use HTTPS**: Use the more secure HTTPS protocol. This is recommended, but can be disabled if not compatible with the server.
- **Host name**: Enter your host name, fully qualified. For example: myhost.mydomain.net.
- **User name**: Enter the user name or key provided by the dynamic DNS service provider. If the dynamic DNS provider supplies only a key, enter that key for both the **User name** and **Password** fields.
- **Password**: Enter the password or key provided by the dynamic DNS service provider.

Advanced Dynamic DNS Settings

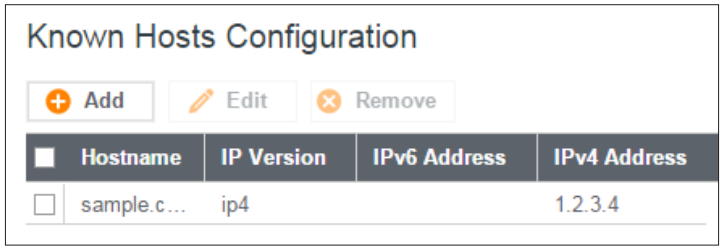
Update period (hours): (Default: 576) The time between periodic updates to the dynamic DNS, if your dynamic IP address has not changed. The timeout period is entered in hours so valid values are from 1 to 8760.

Override External IP: The external IP is usually configured automatically during connection. However, in situations where the unit is within a private network behind a firewall or router, the network's external IP address will have to be manually configured in this field.

You may find out what your external IP address is by going to **http://myip.dnsomatic.com** in a web browser.

Known Hosts Configuration

The Known Hosts Configuration feature allows you to map a name (printer, scanner, laptop, etc.) to an IP address of a device on the network. This assigns a new hostname that can be used to conveniently identify a device within the network, such as an office printer.



©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Click **Add** to name a device in your network.

Fill in the following fields:

- **Hostname**: Choose a name that is meaningful to you. No spaces are allowed in this field.
- **IP address**: The address of the device within your network.

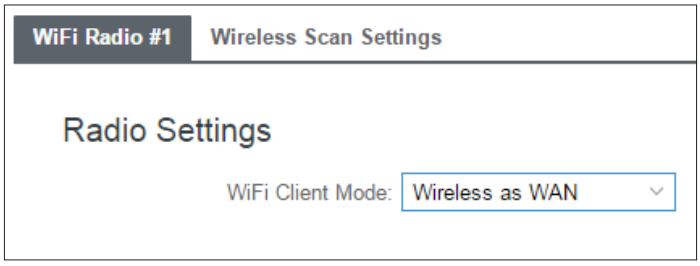
EXAMPLE: a personal laptop with IP address 192.168.0.164 could be assigned the name "MyLaptop."

Since the assigned name is mapped to an IP address, the device's IP address should not change. To ensure that the device keeps the same IP address, go to **NETWORKING > Local Networks > DHCP Server** and reserve the IP address for the device by selecting the device in the **Active Leases** list and clicking **Reserve**.

WIFI AS WAN

WiFi as WAN uses an outside WiFi network as its Internet source. When WiFi as WAN is enabled, the router will find other WiFi networks that you can select and connect to. Unless a selected WiFi source is on an unprotected network, you will need to know its password or key.

To enable WiFi as WAN, select WiFi Radio #1 and **Wireless as WAN** under **WiFi Client Mode**.



All Cradlepoint routers and some other routers use the same default IP address for the primary network: 192.168.0.1. If you attempt to set up WiFi as WAN and there is an "IP conflict," you need to change the IP address. The router is attempting to use the same IP address for both WAN and LAN, which is impossible. Go to **Network Settings > WiFi / Local Networks**. Select the network and click **Edit**. You can change the IP address under **IPv4 Settings**. For example, you might change 192.168.**0**.1 to 192.168.**1**.1.

Saved Profiles

This is a list of WiFi networks that have already been configured as WAN sources. The router will attempt to connect to any of these access points using the password you have configured. If more than one access point is in range, then the router will connect with the highest priority network.

Network: The name (SSID, or Service Set Identifier) that is broadcast by the access point.

BSSID: The numeric ID of the network (Basic Service Set Identifier). This parameter is required when trying to connect to a hidden network using WiFi as WAN. It is optional when connecting to a visible network. If it is set in a profile, both the SSID and BSSID must match to connect to an access point. If the BSSID is not set in a profile, then the router will connect to any access point that matches the given SSID.

Auth Mode: The type of encryption that is used by the network.

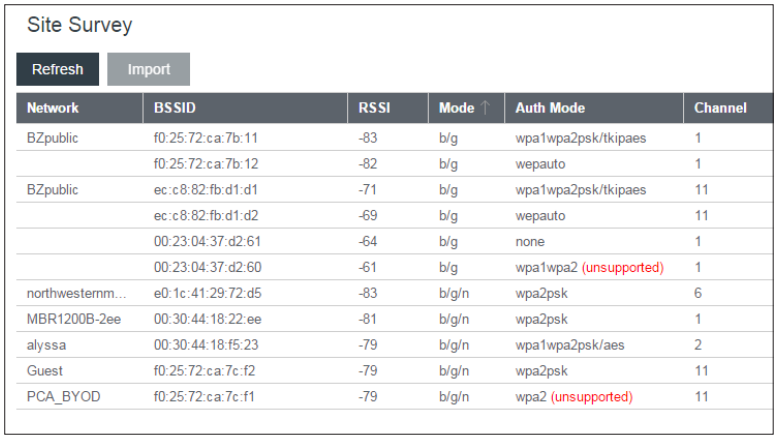
- None
- WEP Auto
- WEP Open

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

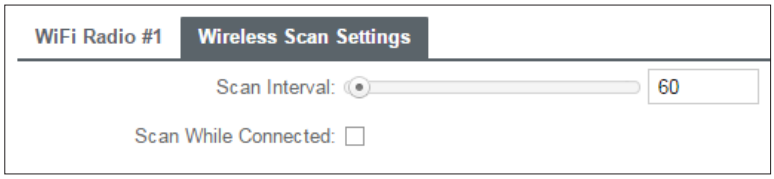
- WEP Shared
- WPA1 Personal
- WPA2 Personal
- WPA1 & WPA2 Personal

You have two options for adding network profiles:

- **Automatic** – Select a WiFi network in **Site Survey** and click **Import**
- **Manual** – Click on **Add** under **Saved Profiles** and input the required information.



Site Survey
This is a list of WiFi networks that the router can currently find, along with information about the network such as its mode and channel. Click "Refresh" if a WiFi network you want to connect to is not listed. You can sort the list based on any of the fields by clicking on the field name.



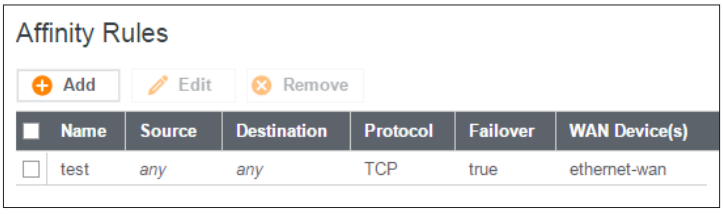
If you import a network from **Site Survey**, most of the information about the network will already be completed. You need to input the password (if there is one) and then click submit to save the WiFi as WAN profile.

Wireless Scan Settings
Scan Interval: How often WiFi as WAN scans the environment for updates. (Default: 60 seconds. Range: 5–3600 seconds.)

Scan While Connected: Continue to scan for WiFi as WAN profile updates when connected. Each time a scan occurs the wireless communication of the router will be temporarily interrupted. Normally this should be disabled.

WAN AFFINITY

WAN Affinity rules allow you to manage traffic in your network so that particular bandwidth uses are associated with particular WAN sources. This allows you to prioritize bandwidth.



EXAMPLE: You could specify that your guest LAN is only associated with your Ethernet connection with no failover. Then if your Ethernet connection goes down and the embedded modem connects for failover for your primary LAN, your guest LAN will not take bandwidth from your primary LAN, saving you money.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Click **Add** to open the WAN Affinity Policy Editor and create a new WAN Affinity rule.

Name: Give a name for your rule that is meaningful to you.

DSCP (DiffServ): Differentiated Services Code Point is the successor to TOS (Type of Service). Use this field to select traffic based on the DSCP header in each IP packet. This field is sometimes set by latency sensitive equipment such as VoIP phones. If you know specific DSCP values, you can input one here.

DSCP Negate: When checked this rule will match on any packet that does NOT match the DSCP field.

Protocol: Select from the dropdown list to specify the protocol for a particular data use. Otherwise, leave "Any" selected.

- Any
- ICMP
- TCP
- UDP
- GRE
- ESP
- SCTP

Source IP Address, **Source Netmask**, **Destination IP Address**, and **Destination Netmask**: Specify an IP address or range of IP addresses by combining an IP address with a netmask for either "source" or "destination" (or both). Source vs. destination is defined by traffic flow. Leave these blank to include all IP addresses (such as if your rule is defined by a particular port instead).

EXAMPLE: If you want to associate this rule with your guest LAN, you could input the IP address and netmask for the guest LAN here (leaving the last slot "0" to allow for any user attached to the guest network):

- **Source IP Address:** 192.168.10.0
- **Source Netmask:** 255.255.255.0

Failover: (Default: Selected.) When this is selected and traffic from the chosen WAN device for this rule is interrupted, the router will fail over to another available WAN device. Deselect this option to restrict this traffic to only the selected WAN interface.

When	Condition	Value
Port	Is	USB Port 1
Type	Is not	WiMax

- **When**:
  - **Port** – Select by the physical port on the router that you are plugging the modem into (e.g., "USB Port 2").
  - **Manufacturer** – Select by the modem manufacturer (e.g., "Cradlepoint Inc.").
  - **Model** – Set your rule according to the specific model of modem.
  - **Type** – Select by type of Internet source (Ethernet, LTE, Modem, Wireless as WAN, WiMAX).
  - **Serial Number** – Select a 3G or LTE modem by the serial number.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

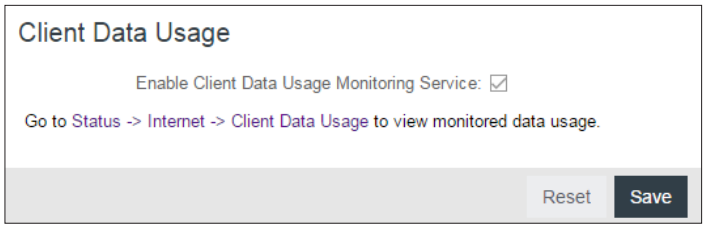
  - **MAC Address** – Select from a dropdown list of attached devices.
  - **Unique ID** – Select by ID. This is generated by the router and displayed when the device is connected to the router.
- **Condition**: Select "is," "is not," "starts with," "contains," or "ends with" to create your condition's statement.
- **Value**: If the correct values are available, select from the dropdown list. You may need to manually input the value.

Load Balance Algorithm: Select the Load Balance Algorithm for this WAN Affinity rule from the following dropdown options:

- **Round-Robin**: Evenly distribute each session to the available WAN connections.
- **Rate**: Distribute load based on the current upload and download rates. A WAN device's upload and download bandwidth values can be set in **CONNECTION MANAGER**.
- **Spillover**: This was the default algorithm in older (version 3) firmware. Load is always given to devices with the most available bandwidth. The estimated bandwidth rate is based on a combination of the upload and download configuration values and the observed capabilities of the device.
- **Data Usage**: This mode works in concert with the Data Usage feature. The router will make a best effort to keep data usage between interfaces at a similar percentage of the assigned data cap in the data usage rule for each interface, rather than distributing sessions based solely on bandwidth. For proper functioning you need to create data usage rules for each WAN device you will be load balancing. Make certain to select the "Use with Load Balancing" checkbox in the data usage rule editor.

CLIENT DATA USAGE

Client Data Usage displays upload and download traffic for each LAN client. Click **Enable Client Data Usage Monitoring Service** to begin tracking this information. This data is not retained between router reboots.


Client Data Usage
Enable Client Data Usage Monitoring Service:
Go to Status -> Internet -> Client Data Usage to view monitored data usage.
Reset
Save

For each client this shows: Name, IP address, MAC address, amount of data uploaded (MB), amount of data downloaded (MB), and when traffic was last sent or received for that client ("Last Traffic").

The names that are shown are received during a DHCP exchange. If a client disconnects and reconnects with a new IP address there will be an additional entry in this list.

Pressing **Reset Statistics** will restart all counters at 0.

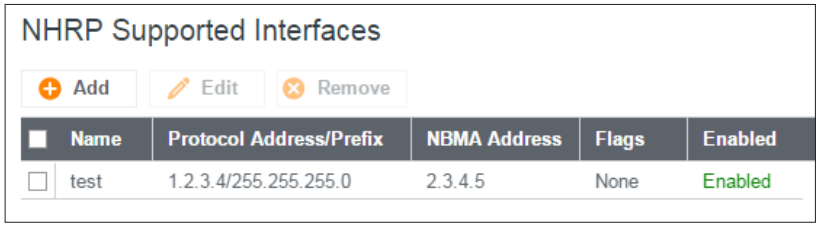
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

NHRP

Next Hop Resolution Protocol is a protocol used to discover addresses of clients on Non-Broadcast Multiple Access (NBMA) networks. It is used to create next-generation VPN technologies that allow shortcutting between spokes. With NHRP, systems attached to an NBMA network dynamically learn the NBMA address of the other systems that are part of that network, allowing these systems to directly communicate without requiring an intermediate hop.

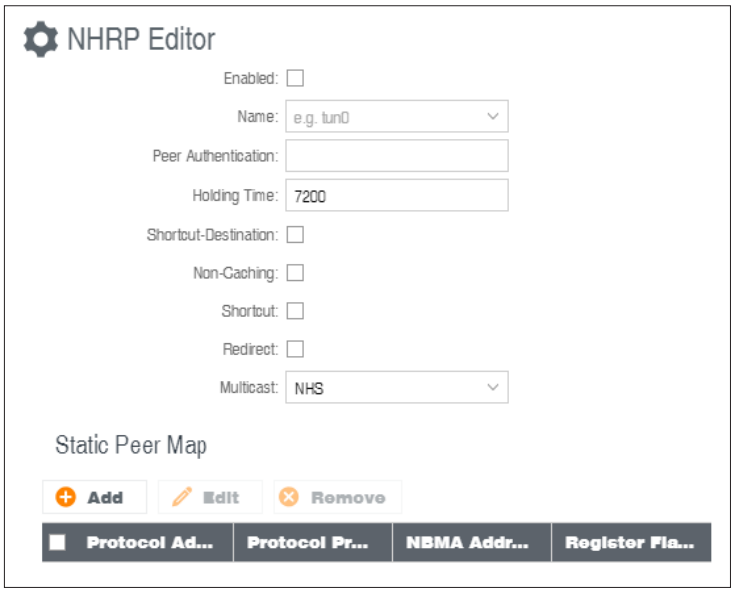
The NHRP Supported Interfaces table displays the following fields for each configured NHRP interface:

- **Name**: Name of the GRE tunnel that NHRP will use
- **Protocol Address/Prefix**: GRE tunnel endpoint mapping that NHRP associates with the NBMA server
- **NBMA Address**: NBMA server address the protocol address/prefix is associated with
- **Flags**:
  - **SD**: Shortcut-Destination
  - **N**: Non-Caching
  - **S**: Shortcut
  - **R**: Redirect



Click **Add** to create a new NHRP interface.

- **Enabled**: Enable or disable the interface.
- **Name**: Give the interface a unique name that matches the mGRE (multipoint GRE) tunnel. Select from configured GRE tunnels or input manually.
- **Peer Authentication**: Embeds the secret plaintext password to outgoing NHRP packets. Incoming NHRP packets on this interface are discarded unless this password is present. Max length: eight characters.
- **Holding Time**: Specifies the holding time for NHRP registration requests and resolution replies.
- **Shortcut-Destination**: Reply with authoritative answers on NHRP resolution requests destined to addresses in this interface (instead of forwarding the packets).
- **Non-Caching**: Disables caching of peer information from forwarded NHRP resolution reply packets.
- **Shortcut**: Enable creation of shortcut routes.
- **Redirect**: Enable sending of proprietary enterprise-style NHRP traffic indication packets.
- **Multicast:** Determines how multicast packets should be forwarded through NHRP interfaces.
  - **NHS:** Multicast packets will be forwarded to each statically configured next hop server. This is default and is typical for the configuration of an NHRP spoke.
  - **Dynamic:** Multicast packets will be forwarded to each connected peer. This is typically used for an NHRP hub.



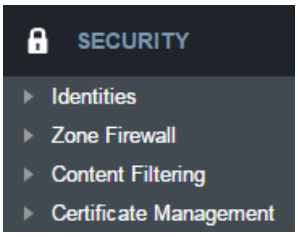
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

You also have the option to create static mappings for this interface. Click **Add** in the table to open the static mapping editor.

- **Protocol Address**: Mapped endpoint to from protocol address to NBMA address
- **Protocol Prefix**: Optional prefix for protocol address
- **NBMA Address**: Destination mapped address from protocol address/prefix
- **Register**: This optional parameter specifies that a **Registration Request** should be sent to this peer on startup (displays flag **R** in the static mapping table if selected)
- **Proprietary OS**: This should be enabled if the statically mapped peer is running proprietary OS (displays flag **C** in the static mapping table if selected).

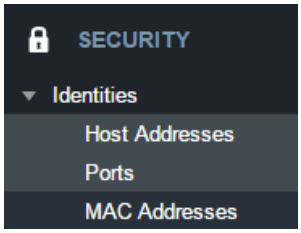
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

SECURITY



IDENTITIES

Identities are reusable groups of items that are added to filter policy rules. A match on any single item in the group will cause the rule to match. Identities are referenced in rules by their name. Choosing descriptive names like “NW Sales Team” or “Engineering” will aid in understanding existing rules and in choosing identities for new rules.



HOST ADDRESSES

A Host identity can contain IPv4, IPv6, and Fully Qualified Domain Name addresses. A single identity can contain a combination of IPv4 and IPv6 addresses. IPv4/6 addresses cannot be combined with FQDN addresses in the same identity.

IP addresses are entered using CIDR notation, e.g. 1.2.3.4/32 and 0123:4567::CDEF/128. FQDN addresses are entered with at least one dot separating a top-level domain from a root zone, e.g. cradlepoint.com.

To add a Host Address Identity, click **Add**.

PORTS

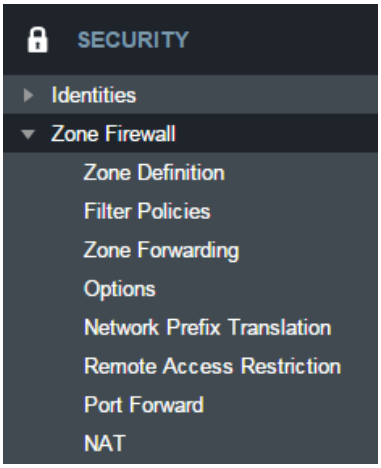
A port identity member can be entered as a single Start port number or as a port range by entering both a Start and End port number.

To add a Port Identity, click **Add**.

MAC ADDRESSES

MAC addresses are entered in the form aa:bb:cc:dd:ee:ff.

To add a MAC Address Identity, click **Add**.



ZONE FIREWALL

ZONE DEFINITION

A Zone is a group of network interfaces. By default all interfaces within a zone are allowed to initialize network communication with each other, however any network traffic initialized outside of a zone to the interfaces within the zone will be denied.

To add a zone, click **Add**.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

FILTER POLICIES

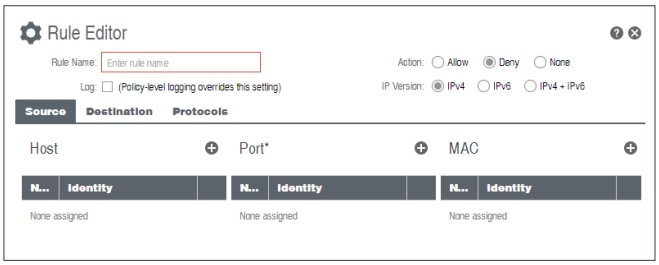
A Filter Policy is a one-way filter applied to initialized network traffic flowing from one zone to another. A Filter Policy needs to be assigned to a Forwarding for it to take effect. Filter Policies can either be Added, Edited, or Removed.

- **Default Allow All** is a preconfigured policy to allow all traffic initialized from one zone to flow to another zone. The state of the connection is tracked to allow responses to traverse the zones back to the source. LAN to WAN forwardings use this policy by default. The policy can be removed or altered to filter the traffic flow.
- **Default Deny All** is a preconfigured policy to deny all traffic initialized from one zone to be blocked to another zone. WAN to LAN forwardings use this policy by default. The policy can be removed or altered to filter the traffic flow.

Click **Add** to create a new filter policy, or select an existing policy and click Edit to open the filter policy editor.

- **Name**: Create a name meaningful to you.
- **Action**: Choose either **Allow** or **Deny**. This is the action taken by the firewall if none of the filter policy rules match the traffic being filtered.
- **Log**: When checked, every rule in the policy will log matching packets as if the rule's Log option had been selected.

Click **Add** to create a new rule for this filter policy, or select an existing rule and click Edit to open the Rule Editor.

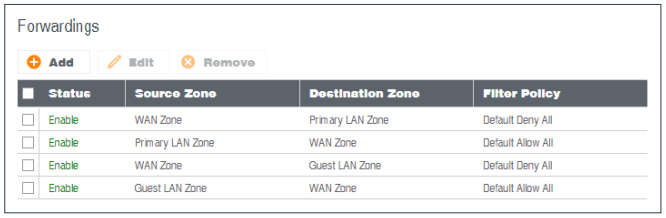


- **Name**: Create a rule name meaningful to you.
- **Action**: Choose either Allow or Deny. This is the action taken by the firewall if the rule criteria match the traffic being filtered.
- **Log**: When checked, each packet matching this filter rule will be logged in the System Log.
- **IP Version**: Select the IP version to match.
- Enter match criteria under **Source**, **Destination**, and **Protocols**.
  - **Source**: Select defined identities or enter individual criteria for the appropriate **Host**, **Port** and **MAC** address columns to match the source of the traffic.
    - **Host**: Enter an IP address or select a host identity.
    - **Port**: Enter a port, port range, or select a port identity.
    - **MAC**: Enter a MAC address or select a MAC address identity.
  - **Destination**: Select defined identities or enter individual criteria for the appropriate Host, Port and MAC address columns to match the destination of the traffic. See **Source** for the column definitions.
  - **Protocols**: Select protocols (such as TCP, UDP, GRE, etc) from the defined list or enter a numeric code for other protocols to match traffic of that protocol.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

ZONE FORWARDING

Forwardings define how Filter Policies affect traffic flowing between zones in one direction. Simply configure the Source Zone, Destination Zone, and Filter Policy to define a Forwarding. Forwardings can be Added, Edited, Removed, or Toggled. Toggling a Forwarding will either enable or disable the Forwarding.



Source and Destination zones are chosen from the list of Zone Definitions. In addition, two special zones can be selected for forwarding endpoints:

- The **All** zone will match any traffic handled by the router and is used as an endpoint for IP Filter Rules migrated from previous firmware versions. User editable zones are preferred when adding new forwardings.
- The **Router** zone will match any traffic initialized from or directed to router services and can be used to filter router service traffic. An example of traffic initialized by a router service would be the NCM service. An example of traffic destined to a router service would be the SNMP service.

OPTIONS

Firewall Options

- **Anti-Spoof**: Anti-Spoof checks help protect against malicious users faking the source address in packets they transmit in order to either hide themselves or to impersonate someone else. Once the user has spoofed their address they can launch a network attack without revealing the true source of the attack or attempt to gain access to network services that are restricted to certain addresses.
- **Log Web Access**: Enable this option to create a syslog record of web (IP port 80) access. Each entry will contain the the IP address of the server and the client. Note that this may create a lot of log entries, especially on a busy network. Sending the system log to a syslog server is recommended.

Application Gateways

Enabling an application gateway makes pinholes thru the firewall. This may be required for some applications to function, or for an application to improve functionality or add features.

NOTE: Exercise caution in enabling application gateways as they impact the security of your network.

- **PPTP**: For virtual private network access using Point to Point Tunneling Protocol.
- **SIP**: For Voice over IP using Session Initiation Protocol.
- **TFTP**: Enables file transfer using Trivial File Transfer Protocol.
- **FTP**: To allow normal mode when using File Transfer Protocol. Not needed for passive mode.
- **IRC**: For Direct Client to Client (DCC) transfer when using Internet Relay Chat. You may wish to forward TCP port 113 for incoming identd (RFC 1413) requests.

DMZ (Demilitarized Zone)

A DMZ host is effectively not firewalled in the sense that any computer on the Internet may attempt to remotely access network services at the DMZ IP address. Typical uses involve running a public web server, supporting older games, or sharing files.

NOTE: As with port forwarding, caution should be used when enabling the DMZ feature as it can threaten the security of your network.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

NETWORK PREFIX TRANSLATION

Network Prefix Translation is used in IPv6 networks to translate one IPv6 prefix to another. **IPv6 prefix translation** is an experimental specification (**RFC 6296)** trying to achieve address independence similar to NAT in IPv4. Unlike NAT, however, NPT is stateless and preserves the IPv6 principle that each device has a routable public address. But it still breaks any protocol embedding IPv6 addresses (e.g. IPsec) and is generally not recommended for use by the IETF. NPT can help to keep internal network ranges consistent across various IPv6 providers, but it cannot be used effectively in all situations.

The primary purpose for Cradlepoint's NPT implementation is for failover/failback and load balancing setups. LAN clients can potentially retain the original IPv6 lease information and may experience a more seamless transition when WAN connectivity changes than if not utilizing NPT.

Mode:

- **None** – No translation is performed
- **Load Balance Only** – (Default) Only translate networks when actively load balancing
- **First** – Use the first IPv6 prefix found
- **Static** – Always use a static IPv6 translation (input the prefix here)

Transitioning from short prefix to a longer prefix (such as from /48 to /64) is not without problems, as some of the LANs may lose IPv6 connectivity.

REMOTE ACCESS RESTRICTION

Add any IPv4 addresses that need access to remote administration to this list. Clicking **Add** will allow the addition of IP address and netmask pairs to the administration filter. **Edit** will allow you to change settings for the selected address. **Remove** will remove a selected entry.

PORT FORWARD

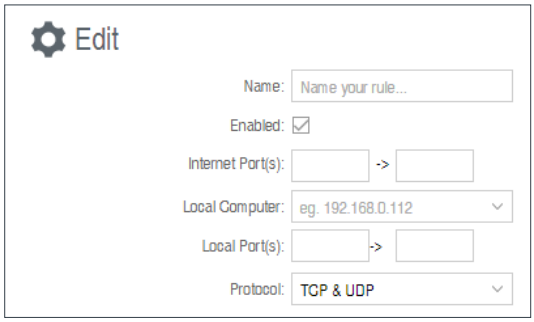
A port forwarding rule allows traffic from the Internet to reach a computer on the inside of your network. For example, a port forwarding rule might be used to run a Web server.

NOTE: Exercise caution when adding new rules as they impact the security of your network.

Click **Add** to create a new port forwarding rule, or select an existing rule and click **Edit**.

Add/Edit Port Forwarding Rule

- **Name**: Name your rule.
- Enabled: Toggle whether your rule is enabled. Selected by default.
- **Use Port Range**: Changes the selection options to allow you to input a range of ports (if desired).
- **Internet Port(s)**: The port number(s) as you want it defined on the Internet. Typically these will be the same as the local port numbers, but they do not have to be. These numbers will be mapped to the local port numbers.



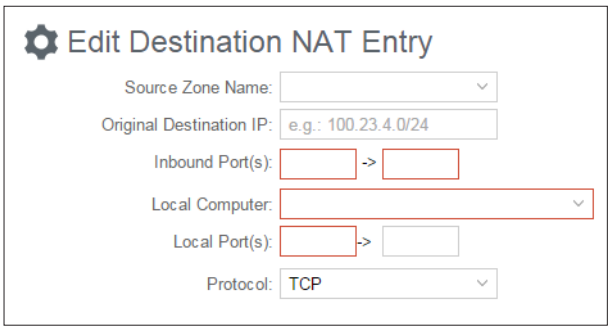
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- **Local Computer**: Select the IP address of an attached device from the dropdown menu, or manually input the IP address of a device.
- **Local Port(s)**: The port number(s) that corresponds to the service (Web server, FTP, etc.) on a local computer or device. For example, you might input "80" in the Local Port(s) field to open a port for a Web server on a computer within your network. The Internet Port(s) field could then also be 80, or you could choose another port number that will be used across the Internet to access your Web server. If you choose a number other than 80 for the Internet Port, connections to that number will be mapped to 80 – and therefore the Web server – within your network.
- **Protocol**: Select from the following options in the dropdown menu:
  - **TCP**
  - **UDP**
  - **TCP & UDP**

Click **Save** to save your completed port forwarding rule.

NAT

Zone NAT is similar to Port Forwarding and provides that functionality by mapping ports available on interfaces associated with the Zone to ports available on local clients. Zone NAT also has the ability to map many types interfaces selectable via a Zone. For example, GRE interfaces can be used to port forward traffic from the GRE endpoints to local client thereby limiting exposure to the local LAN while still gaining the benefits of GRE.

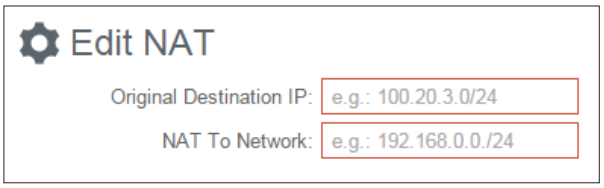


Click **Add** to create a Destination NAT.

- **Source Zone Name:** The Zone created in Zone Firewall. Select the Zone to NAT.
- **Original Destination IP:** Specify which inbound traffic to this router will have the destination IP translated to an internal network.
- **Inbound Port(s):** Specify the IP port(s) on the inbound traffic to forward to a local computer.
- **Local Computer:** Specify the local computer to receive forwarded traffic.
- **Local Port(s):** Specify the IP port (first if a range) on the local computer to receive forwarded traffic.
- **Protocol:** Select the IP protocol traffic to forward.

NAT

NAT allows translating the destination ip of incoming network traffic to a local network. All ports and protocols will be forwarded. Netmasks should generally match. If the local network range is larger than the incoming destination range then network traffic will begin using port overloading. One-to-One NAT can be accomplished by specifying a host address or a /32 cidr address.



Click **Add** to create a NAT.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

CONTENT FILTERING

WEBFILTER SETTINGS

General Settings

Enbable Webfilter: Selecting "Enable Webfilter" will enable the webfiltering service. This is used to enable or disable all router-based webfiltering and forwarding.

Filter HTTPS: Selecting "Filter HTTPS" enables redirection of all port 443 traffic into the proxy. The proxy will then extract the host name from the SNI (Server Name Indication). If SNI is unavailable then the original destination IP address is used for filtering. No decoding of the SSL/TLS session is done.

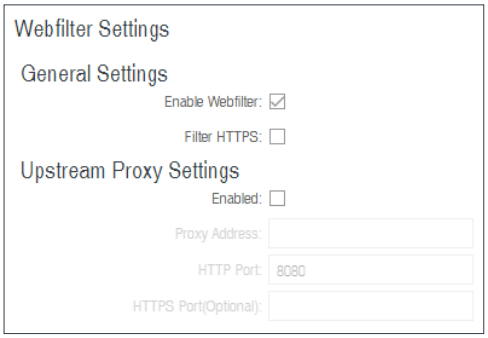
Upstream Proxy Settings

Enabled: Select whether the use of an Upstream Proxy server is enabled.

Proxy Address: The Proxy Address is the address the desired HTTP proxy is hosted at. Addresses can be input as host names or as ip addresses. If the proxy is unavailable HTTP traffic will fail to cross the network and a notification page will be shown.

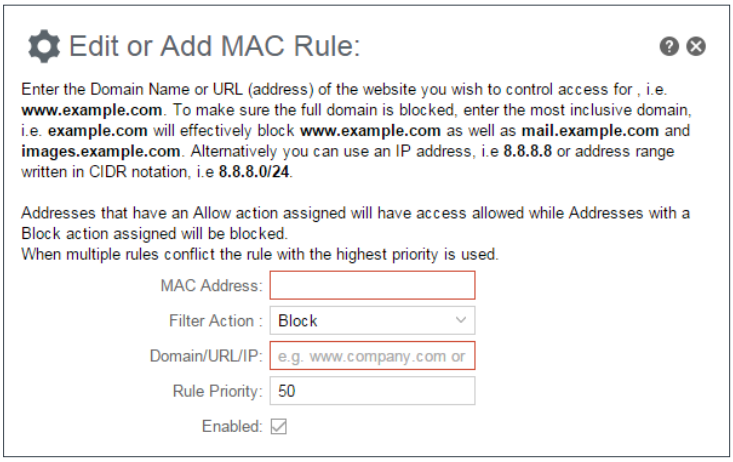
HTTP Port: The port the HTTP Proxy is listening on.

HTTPS Port (Optional): The port for the proxy to forward HTTPS traffic to. HTTPS is not transparently intercepted and must have the LAN clients configured to use the Cradlepoint router as a proxy for HTTPS to work properly.



MAC WEB FILTER RULES

MAC Address WebFilter Rules allow you to control access from a specific MAC address to external domains or websites. To add a rule, click **Add**.


Edit or Add MAC Rule:
Enter the Domain Name or URL (address) of the website you wish to control access for , i.e. www.example.com. To make sure the full domain is blocked, enter the most inclusive domain, i.e. example.com will effectively block www.example.com as well as mail.example.com and images.example.com. Alternatively you can use an IP address, i.e 8.8.8.8 or address range written in CIDR notation, i.e 8.8.8.0/24.
Addresses that have an Allow action assigned will have access allowed while Addresses with a Block action assigned will be blocked.
When multiple rules conflict the rule with the highest priority is used.
MAC Address:
Filter Action : Block
Domain/URL/IP: e.g. www.company.com or
Rule Priority: 50
Enabled:

- **MAC Address**: Enter MAC Address.
- **Filter Action**: Select Block or Allow.
- **Domain/URL/IP**: Enter the Domain Name or URL (address) of the website you wish to control access for, e.g. www.google.com. To make sure the full domain is blocked, enter the most inclusive domain (e.g. google.com will effectively block www.google.com as well as maps.google.com and images.google.com). Alternatively you can use an IP address, e.g. 8.8.8.8, or address range written in CIDR notation, e.g. 8.8.8.0/24.
- **Rule Priority**: Higher number rules overrule lower number rules.
- **Enabled**: A rule can be enabled or disabled by selecting or deselecting the checkbox.

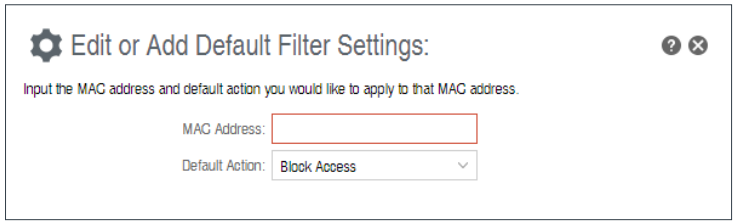
Use **MAC Address WebFilter Defaults** together with **MAC Address WebFilter Rules** to control website access for specific MAC addresses. By default, each MAC address is allowed website access. Click **Add/Edit** to change this setting for a MAC address.

Input the **MAC Address** and **Default Action** you would like to apply to that MAC address.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Default Action: Select from the following dropdown options:

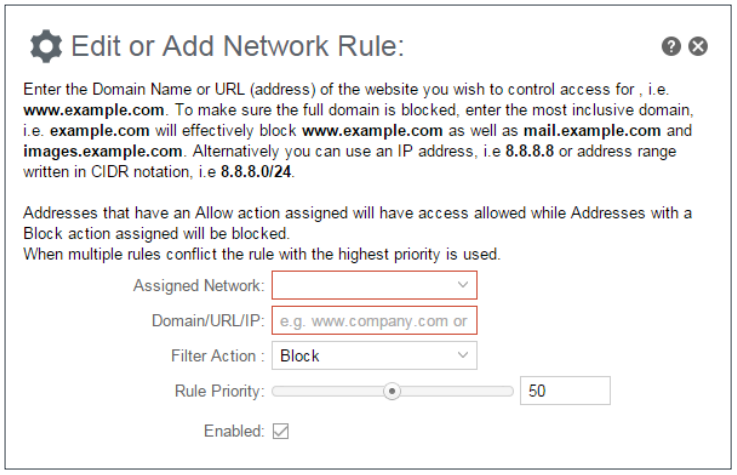
- Allow Access (default)
- Block Access


Edit or Add Default Filter Settings:
Input the MAC address and default action you would like to apply to that MAC address.
MAC Address:
Default Action:
Block Access

When a network is set to **Allow Access**, it will allow access to sites not specifically blocked in the WebFilter Rules. When a network is set to **Block Access**, it will block access to sites not specifically allowed in the WebFilter Rules.

NETWORK WEB FILTER RULES

Domain / URL filter rules allow you to control access from your network to any external domain or website. Rules are assigned to a specific LAN network and the highest priority rule will have precedence when there is a conflict. Addresses can be added by URL/Domain name or by IP address. IP address ranges can be filtered by using CIDR notation, e.g. 4.2.2.2/24.


Edit or Add Network Rule:
Enter the Domain Name or URL (address) of the website you wish to control access for , i.e. www.example.com. To make sure the full domain is blocked, enter the most inclusive domain, i.e. example.com will effectively block www.example.com as well as mail.example.com and images.example.com. Alternatively you can use an IP address, i.e 8.8.8.8 or address range written in CIDR notation, i.e 8.8.8.0/24.
Addresses that have an Allow action assigned will have access allowed while Addresses with a Block action assigned will be blocked.
When multiple rules conflict the rule with the highest priority is used.
Assigned Network:
Domain/URL/IP:
e.g. www.company.com or
Filter Action :
Block
Rule Priority:
50
Enabled:

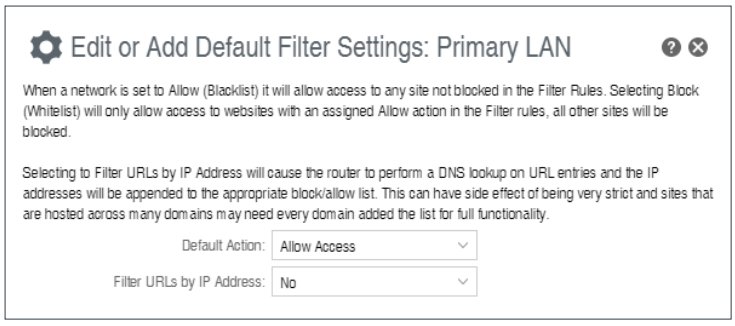
Exceptions to existing rules can be created by adding another rule with higher priority. For example if access to maps.example.com is desired, but example.com is blocked with a priority of 50. The addition of an allow rule for maps.example.com with a priority of 49 or less will allow access.

When creating rules keep in mind that some sites use multiple domains so each domain may need a rule added to produce the desired behavior.

To add a Network Web Filter Rule, click **Add**.

Default Network Filter Settings

When a network is set to Allow (Blacklist) it will allow access to those sites not blocked in the Filter Rules. Selecting Block (Whitelist) will only allow access to websites with an Allow action in the Filter rules, all other sites will be blocked.


Edit or Add Default Filter Settings: Primary LAN
When a network is set to Allow (Blacklist) it will allow access to any site not blocked in the Filter Rules. Selecting Block (Whitelist) will only allow access to websites with an assigned Allow action in the Filter rules, all other sites will be blocked.
Selecting to Filter URLs by IP Address will cause the router to perform a DNS lookup on URL entries and the IP addresses will be appended to the appropriate block/allow list. This can have side effect of being very strict and sites that are hosted across many domains may need every domain added the list for full functionality.
Default Action:
Allow Access
Filter URLs by IP Address:
No

Selecting to Filter URLs by IP Address will cause the router to perform a DNS lookup on URL entries and the IP addresses will be appended to the appropriate block/allow list. This can have side effect of being very strict and sites that are hosted across many domains may need every domain added the list for full functionality.

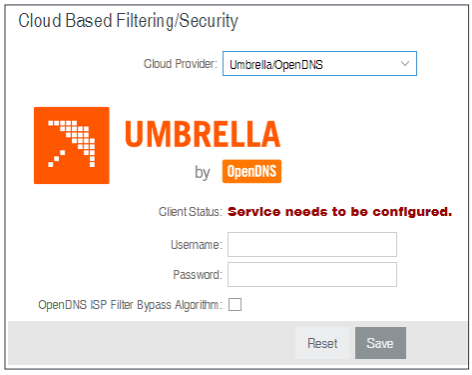
The settings can be changed by selecting a network and clicking the **Edit** button.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

CLOUD-BASED FILTERING

Select a third-party **Cloud Provider** from the dropdown list.

- **Umbrella** by **OpenDNS**
- **Zscaler Secure Web Gateway**
- **Zscaler Internet Security**

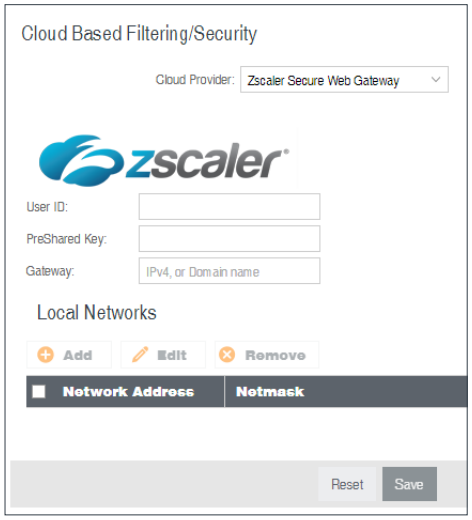


Umbrella by OpenDNS

Umbrella by OpenDNS is a cloud-based web filtering and security solution that protects you online by filtering websites. Go to **http://www.opendns.com/business-security** for information about Umbrella.

Enter your Umbrella account information in order to use these content filtering settings.

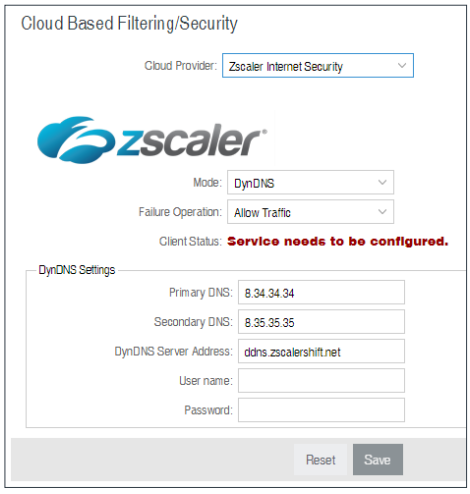
OpenDNS ISP Filter Bypass Algorithm: It is possible that your Internet Service Provider (ISP) uses the port that OpenDNS is configured to access, port 53, which will prevent OpenDNS filtering. If OpenDNS does not appear to be working correctly, enabling this will attempt to bypass those ports when using an OpenDNS content filtering level.



Zscaler

Zscaler is a cloud-based web filtering and security provider that offers several plan options. Depending on your Zscaler implementation, this could include:

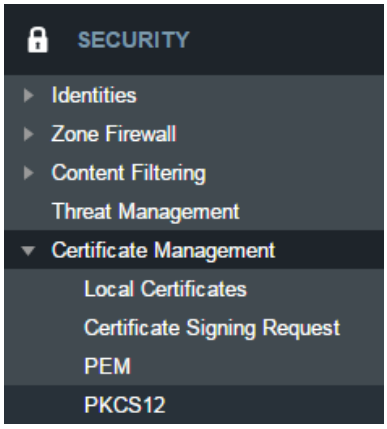
- Global Cloud Platform
- Real-Time Reporting
- Behavioral Analysis
- URL Filtering
- Advanced Threat Protection
- Inline Anti-Virus & Anti-Spyware
- Web 2.0 Control
- Data Loss Prevention
- Bandwidth Management
- Web Access Control
- And more...



NOTE: Zscaler requires a feature license. Go to **SYSTEM > Feature Licenses** to enable this feature.

Enter your Zscaler account information to enable these settings. Input local network information (Network Address and Netmask) to assign your Zscaler implementation to one or more local network(s).

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com



CERTIFICATE MANAGEMENT

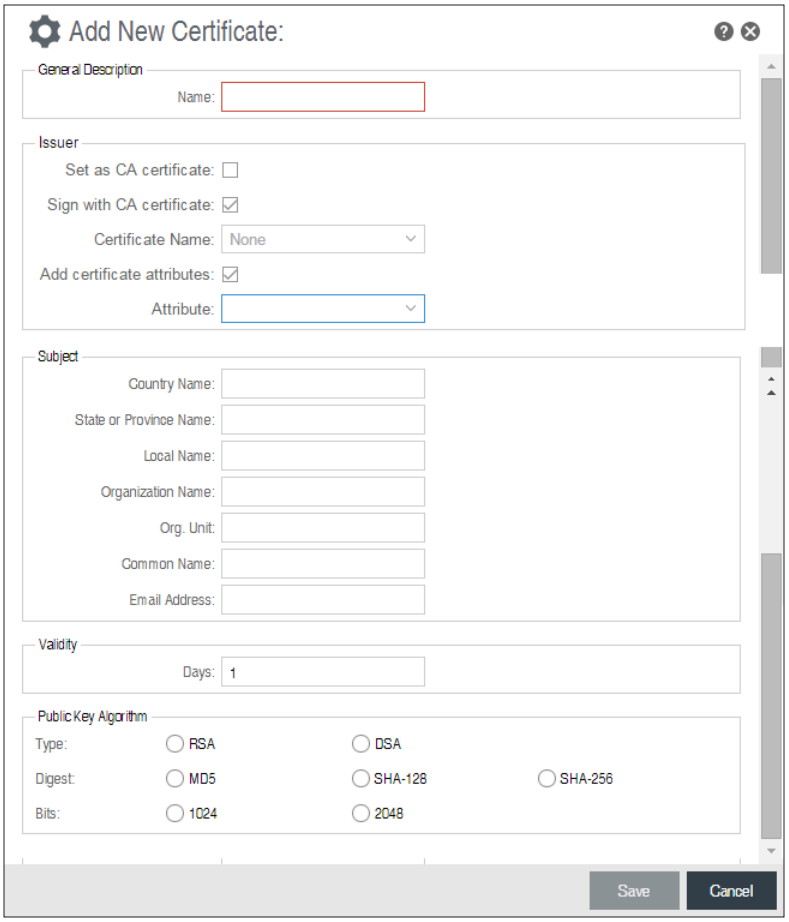
LOCAL CERTIFICATES

This is a table of local certificates, including certificate details.

- **Name**: Friendly description of the certificate.
- **Location**: The certificate issuer's locality (city, town, etc.)
- **Organization Information**: The organization to which the certificate issuer belongs
- **Common Name**: Name used to match authentication credentials

To add a local certificate, click **Add**.

Remove a local certificate by selecting the certificate and clicking the **Remove** button.



©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

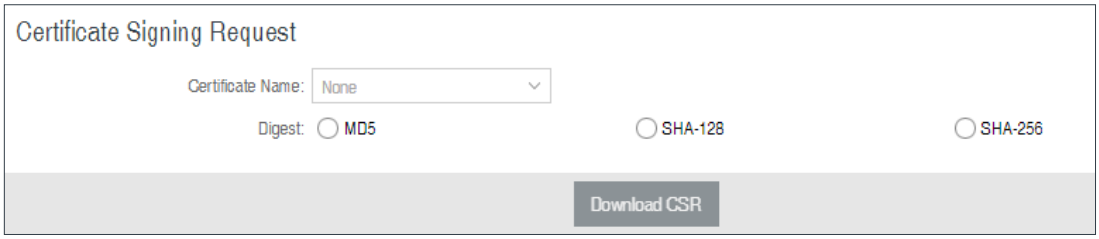
CERTIFICATE SIGNING REQUEST

Request a certificate signature from a remote CA. Using an established, third-party CA increases the likelihood that your certificate will be trusted by others (see **security issues** for self-signed certificates for more information).

Generate a **certificate signing request** (CSR) by selecting a certificate from the dropdown list (**Certificate Name** field) and downloading the CSR. The CSR can then be sent to a remote CA for a signature. Once the certificate has been signed, import the certificate in PEM or PKCS #12 format.

When you export the CSR, select a **Digest**, or **cryptographic hash function**. These are listed in order of increasing security. More security requires more router resources.

- **MD5**
- **SHA-128**
- **SHA-256**



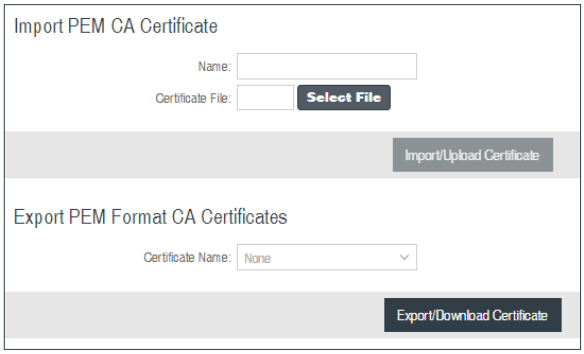
PEM

PEM is a container format for encoding data – in this case, X.509 certificates. PEM was originally designed for encoding email (PEM stands for **Privacy-enhanced Electronic Mail**), but it has never been widely used for that purpose. The format is much more common for encoding digital certificates.

The PEM format uses **Base64** and **DER** (Distinguished Encoding Rules) encoding.

To import, choose a certificate file in PEM format from your computer or local device and upload it to the router. Give the certificate a name that is meaningful to you.

To export, select a local certificate from the dropdown list and download it to your computer or local device in PEM format.



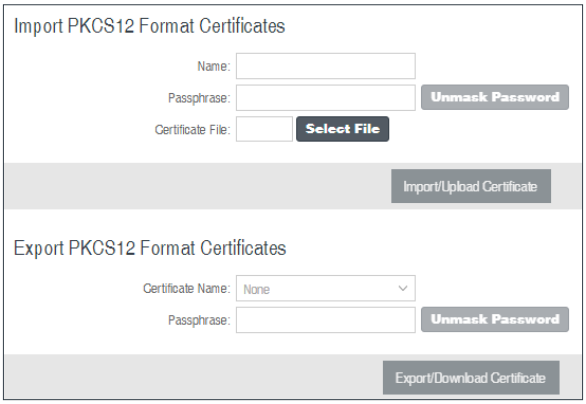
PKCS12

PKCS #12 is one of the **public-key cryptography standards**. PKCS #12 files bundle public and private certificate keys in an archive file format. The PKCS #12 container format is more secure than the PEM container format because it is protected by an encryption key.

To import, choose a certificate file in PKCS #12 format from your computer or local device and upload it to the router. Give the certificate a name that is meaningful to you. PKCS #12 files are protected by a passphrase – you must know this key to import the file.

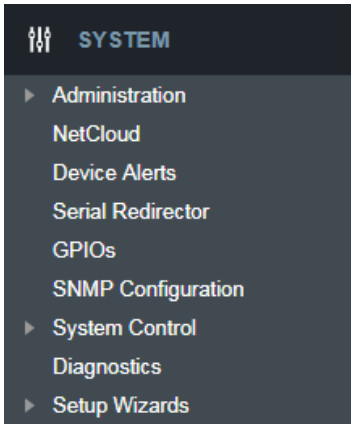
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

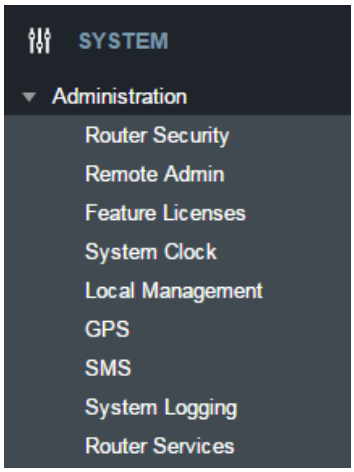
To export, select a local certificate from the dropdown list and download it to your computer or local device in PKCS #12 format. When you export this file, you must create a passphrase to protect it. This key is required for future use of the file.



©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

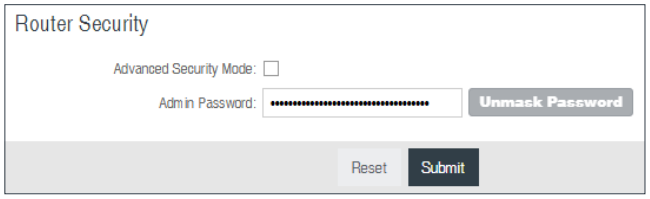
SYSTEM





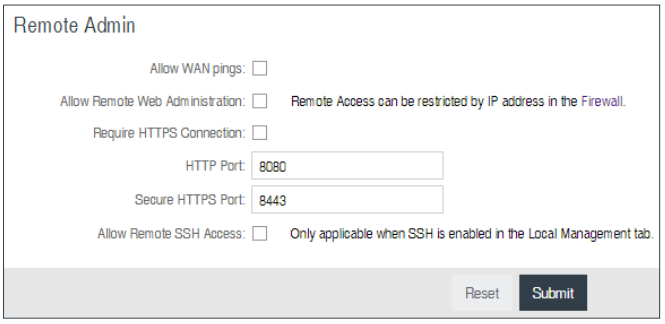
ADMINISTRATION

ROUTER SECURITY



When the router is configured to use the advanced security mode, several aspects of the routers configuration and networking functionality will be extended to support high security environments. This includes support for multiple user accounts, increased password security and additional network spoofing filters. If you plan to use your router in a PCI DSS compliant environment this option is mandatory.

REMOTE ADMIN



Remote Management allows a user to enable incoming WAN pings or change settings for the router from the Internet using the router's Internet address.

Allow WAN pings – When enabled the functionality allows an external WAN client to ping the router.

Allow Remote Web Administration – When remote administration is enabled it allows access to these administration web pages from the Internet. With it disabled, you must be a client on the local network to access the administration website. For security, remote access is usually done via a non-standard http port. Additionally, encrypted connections can be required for an added level of security.

- **Require HTTPS Connection** – Requiring a secure (https) connection is recommended
- **HTTP Port:** Default – 8080. This option is disabled if you select "Require Secure Connection"

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- **Secure HTTPS Port** – Default: 8443.

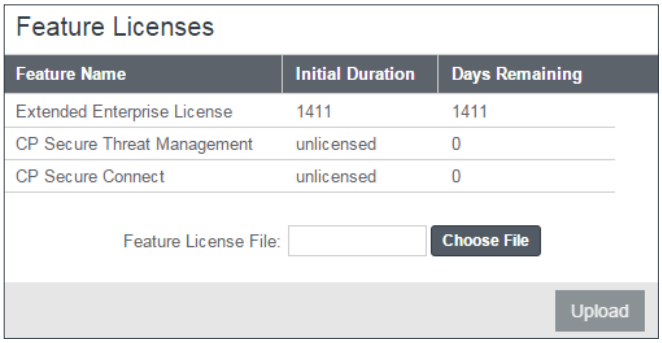
NOTE: You can restrict remote access to only specified IP addresses in **SECURITY > Zone Firewall > Remote Access Restriction**.

Allow Remote SSH Access – This will enable SSH access to the router from the Internet. It is only available when SSH access is enabled in the Local Management tab. Some carriers block the remote SSH access ports. If a ping to the router's WAN port does not work, it is unlikely that remote SSH access will work.

FEATURE LICENSES

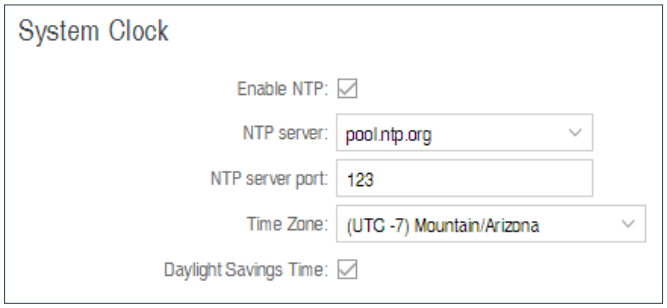
Some Cradlepoint features may require a license. These features are disabled by default. To obtain a feature license, contact your Cradlepoint sales representative.

Once you have obtained the feature license file, upload the file to enable the feature. A reboot is required after uploading a feature license file.



SYSTEM CLOCK

Enabling NTP will tell the router to get its system time from a remote server on the Internet. If you do not enable NTP, the router time will be based on when the router OS was built, which is guaranteed to be wrong. Whenever the Internet connection is re-established and once a week thereafter the router will ask the server for the current time so it can correct itself.



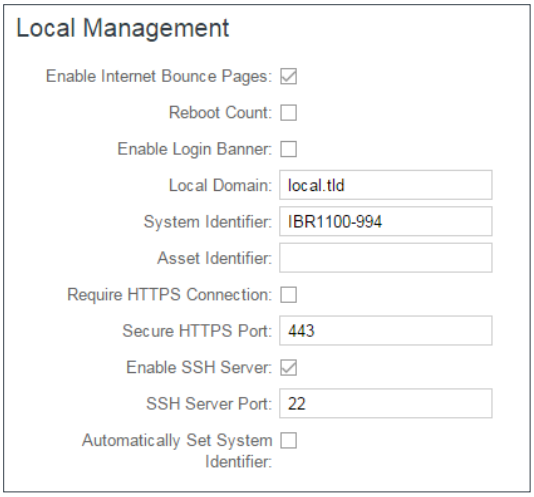
You then have the option of selecting an NTP server and adjusting the NTP server port. Select the NTP server from the dropdown list. Any of the given NTP servers will be sufficient unless, for example, you need to synchronize your router's time with other devices in a network.

- **Time Zone** – Select from a dropdown list. Setting your Time Zone is required to properly show time in your router log.
- **Daylight Savings Time** – Select this checkbox if your location observes daylight saving time.

LOCAL MANAGEMENT

- **Enable Internet Bounce Pages** – Bounce pages show up in your web browser when the router is not connected to the Internet. They inform you that you are not connected and try to explain why. If you disable bounce pages then you will just get the usual browser timeout. In the normal case when the router is connected to the Internet you don't see them at all.
- **Reboot Count** – Track number of router reboots.

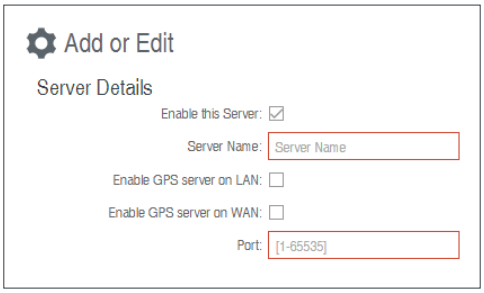
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com



- **Enable Login Banner** – Add the CLI banner to the router's login page.
- **Local Domain** – The local domain is used as the suffix for DNS entries of local hosts. This is tied to the hostnames of DHCP clients as DHCP_HOSTNAME.LOCAL_DOMAIN.
- **System Identifier** – This is a customizable identity that will be used in router reporting and alerting. The default value is the product name and the last three characters of the MAC address of the router.
- **Asset Identifier** – This is a customizable string that will be used in router reporting and alerting.
- **Require HTTPS Connection** – Check this box if you want to encrypt all router administration communication.
- **Secure HTTPS Port** – Enter the port number you want to use. The default is 443.
- **Enable SSH Server** – When the router's SSH server is enabled you may access the router's command line interface (CLI) using the standards-based SSH protocol. Use the username "admin" and the standard system password to log in.
- **SSH Server Port** – Default: 22.
- **Automatically Set System Identifier** – This will automatically set the system ID to the name of the first client that gets a DHCP lease. This feature cannot be used with email alerts but alerts can be sent to NCM.

GPS

If you have an attached device with GPS support, you can enable a graphical view of your router's location, which appears in **STATUS > GPS**. SIM-based models with GPS support require that the SIM be inserted. Some carriers disable GPS support in otherwise supported modems. If you encounter issues with obtaining a fix, contact your carrier and ensure that GPS is supported.



Enable GPS – Enable support for querying GPS information from capable modems.

Send to Client(s)

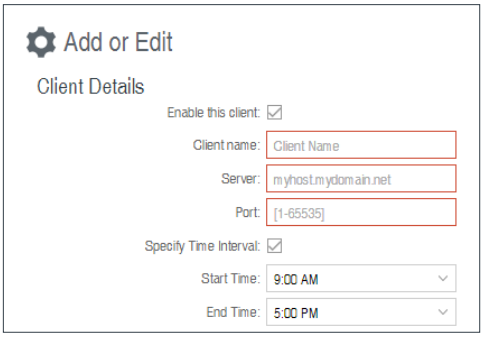
- **Enable this Server** - Enables a local server to which clients can connect and recieve GPS sentences.
- **Server Name** - Your server's name should include only Aa-Zz, numerals, and '_'.
- **Enable GPS server on LAN** - Enables a server on the LAN side of the firewall which will periodically send GPS sentences to TCP connected clients.
- **Enable GPS server on WAN** - Enables a server on the WAN side of the firewall which will periodically send GPS sentences to TCP connected clients.
- **Port** - Choose a port between 1 and 65535.

Send to Server(s)

- **Enable this client** - Enables periodic reporting of GPS sentences to a remote server. The router will buffer GPS sentences if errors are encountered or if the Internet connection goes down, and send the buffered sentences when the connection is restored.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

- **Client name** - Your client's name should include only Aa-Zz, numerals, and '_'.
- **Server** - Remote server hostname or IP.
- **Port** - Remote server port.
- **Specify Time Interval** - Restricts the GPS sentence reporting to a remote server to a specific time interval.
- **Start Time** - Reporting start time.
- **End Time** - Reporting end time.



SMS

SMS (Short Message Service, or text messaging) requires a cellular modem with an active data plan. SMS is not designed to be a full remote management feature: SMS allows you to connect to the router for a few simple queries or commands with a text messaging service (e.g., from your phone). A modem that does not have an active data connection may still be reachable by SMS because Internet traffic and SMS traffic operate on separate channels, so SMS can be used to bring an offline router back online.

SMS
Enable SMS support:
This feature only works if SMS is supported and enabled on the modem. SMS messages are subject to carrier charges based on the texting plan.Contact your carrier to enable SMS and activate an SMS plan.
Password:
Unmask Password
White list
Add
Edit
Remove
SMS Phone number

SMS is enabled on the router by default. However, it only works if SMS is supported and enabled on the modem. Most modems have SMS enabled by default, but the carrier may charge a fee for each text message sent or received. Contact your carrier to review these fees and/or to enable an SMS plan.

Important notes about SMS:

- Messages are limited to 160 characters.
- SMS is not a guaranteed delivery protocol. The carriers do not guarantee that the SMS message will be delivered to the modem or that the modem's response will be delivered to the sender. This means an administrator might have to send messages multiple times before the desired action is performed.
- SMS is a slow protocol. It can take seconds or up to a few minutes for messages to be delivered.
- SMS messages are not encrypted; they are sent in full readable text over the network.

Enable SMS support – SMS support is enabled by default on the router. Deselect this to disable.

Password – By default, the password is the last eight characters of the router's MAC address (i.e., the Default Password on the product label). You can change this password to anything between 1 and 16 characters. It should be long enough to be useful for security but short enough to easily type into your phone (or other texting client).

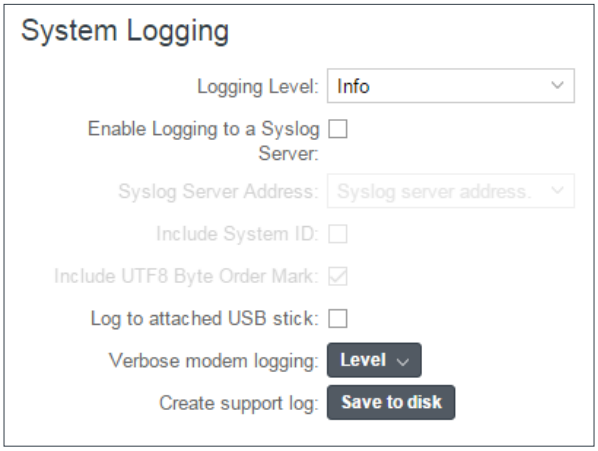
White List – This list is blank by default, which means that the router will accept SMS messages from any phone number. Leaving this blank is unsecure, so Cradlepoint recommends that you add phone numbers to this list. Once any numbers are listed, only those numbers have the ability to connect to the router via SMS.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

SYSTEM LOGGING

Logging Level: Setting the log level controls which messages are stored or filtered out. A log level of **Debug** will record the most information while a log level of **Critical** will only record the most urgent messages. Each level includes all messages from all of the levels below it on the list (e.g. "Warning" includes all "Error" and "Critical" messages as well).

- **Debug**
- **Info**
- **Warning**
- **Error**
- **Critical**



Enable Logging to a Syslog Server: Enabling this option will send log messages to a specified Syslog server. After enabling, type the Hostname or IP address of the Syslog server (or select from the dropdown menu).

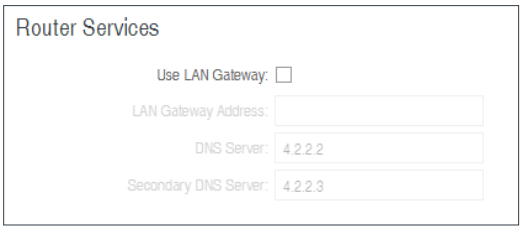
- **Syslog Server Address**: Select the Hostname or IP address from the dropdown menu, or type this in manually.
- **Include System ID**: This option will include the router's "System ID" at the beginning of every log message. This is often useful when a single remote Syslog server is handling logs for several routers.
- **Include UTF8 Byte Order Mark**: The log message is sent using UTF-8 encoding. By default the router will attach the Unicode Byte Order Mark (BOM) to the Syslog message in compliance with the Syslog protocol, RFC5424. Some Syslog servers may not fully support RFC5424 and will treat the BOM as ASCII text, which will appear as garbled characters in the log. If this occurs, disable this option.

Log to attached USB stick: Only enable this option if instructed by a Cradlepoint support agent. This will write a very verbose log file to the root level of an attached USB stick. Please disable the feature before removing the USB stick, or you may lose some logging data.

Verbose modem logging: Only enable this option if instructed by a Cradlepoint support agent.

Create support log: This functionality allows for a quick collection of system logging. Create this log file when instructed by a Cradlepoint support agent.

ROUTER SERVICES



By default, router services (NetCloud Manager, NTP, etc.) connect to the router via the WAN. In some setups it makes sense to use the LAN instead. For example, if your router is used strictly for 3G/4G failover behind another router, you may not want to use 3G/4G data unnecessarily. Select **Use LAN Gateway** to set your router services to connect via the LAN.

LAN Gateway Address: Input the IP address of the LAN side connection. If this is a 3G/4G failover router operating behind another router, the LAN Gateway Address is the IP address of that other router.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

DNS Server and **Secondary DNS Server**: The primary and secondary DNS server numbers match the static DNS values (set at **NETWORKING > DNS Servers**). You can leave the default values or set them manually here. (Changing these values also changes the static DNS values.)

NETCLOUD

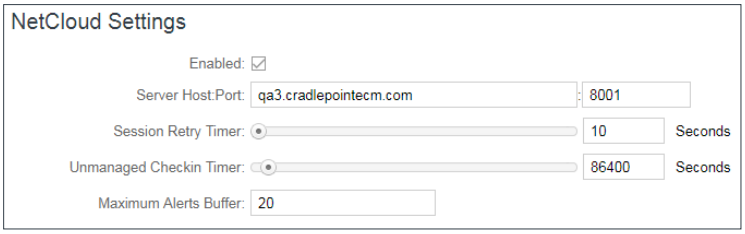
Cradlepoint **NetCloud Manager** (NCM) is a cloud-based management service for configuring, monitoring, and organizing your Cradlepoint routers. Key features include the following:

- Group based configuration management
- Health monitoring of router connectivity and data usage
- Remote management and control of routers
- Historical record keeping of device logs and status

Registering Your Router – Once you have signed up for NCM, click on the Register Router button to begin managing the router through NCM. Input your NCM Username and NCM Password and click Register. You have now registered the device with NetCloud Manager.

Suspending the NCM Client – Click on the Suspend Client button to stop communication between the device and NCM. Suspending the client will make it stop any current activity and go dormant. It will not attempt to contact the server while suspended. This is a temporary setting that will not survive a router reboot; to disable the client altogether use the Advanced NetCloud Settings panel (below).

NetCloud Settings (Advanced)



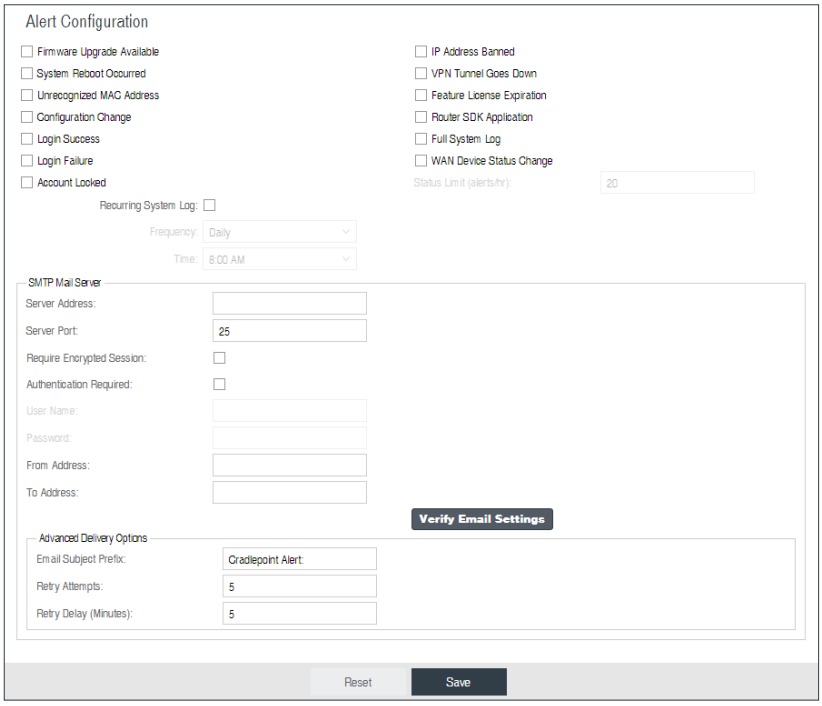
- **Enabled**: Enable the NCM client to contact the server. While this box is unchecked, the NCM client will never attempt to contact the server. (Default: Enabled)
- **Server Host:Port**: The DNS hostname and port number for your NCM server. (Default: stream.cradlepoint.com)
- **Session Retry Timer**: How long to wait, in seconds, before starting a new NCM session following a connection drop or connectivity failure. Note that this value is a starting point for an internal backoff timer that prevents superfluous retries during connectivity loss.
- **Unmanaged Checkin Timer**: How often, in seconds, the router checks with NCM to see if the router is remotely activated. Note that this value is a starting point for an internal backoff timer that reduces network usage over time.
- **Maximum Alerts Buffer**: The maximum number of alerts to buffer when offline.

DEVICE ALERTS

The Device Alerts submenu choice allows you to receive email notifications of specific system events. *YOU MUST ENABLE AN SMTP EMAIL SERVER TO RECEIVE ALERTS.*

Alerts can be included for the following:

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com



- **NCOS Upgrade Available**: An NCOS update is available for this device.
- **System Reboot Occurred**: This router has rebooted. This depends on NTP being enabled and available to report the correct time.
- **Unrecognized MAC Address**: Used with the MAC monitoring lists. An alert is sent when a new unrecognized MAC address is connected to the router.
- **WAN Device Status Change**: An attached WAN device has changed status. The possible statuses are plugged, unplugged, connected, and disconnected.
- **Configuration Change**: A change to the router configuration.
- **Login Success**: A successful login attempt has been detected.
- **Login Failure**: A failed login attempt has been detected.
- **Account Locked**: Account has been locked due to excessive failed login attempts.
- **IP Address Banned**: An IP address has been banned.
- **VPN Tunnel Goes Down**: Sends an alert when a VPN tunnel goes down.
- **Feature License Expiration**: Sends an alert when a feature license is about to expire.
- **Router SDK Application**: A router SDK Application may send an alert.
- **Full System Log**: The system log has filled. This alert contains the contents of the system log.
- **Recurring System Log**: The system log is sent periodically. This alert contains all of the system events since the last recurring alert. It can be scheduled for daily, weekly and monthly reports (**Frequency**). You also choose the **Time** you want the alert sent.

SMTP Mail Server

Since your router does not have its own email server, to receive alerts you must enable an SMTP server. This is possible through most email services (Gmail, Yahoo, etc.)

Each SMTP server will have different specifications for setup, so you have to look those up separately. The following is an example using Gmail:

- **Server Address**: smtp.gmail.com
- **Server Port**: 587 (for TLS, or Transport Layer Security port; the router does not support SSL).
- **Authentication Required**: For Gmail, mark this checkbox.
- **User Name**: Your full email address
- **Password**: Your Gmail password
- **From Address**: Your email address
- **To Address**: Your email address

Once you have filled in the information for the SMTP server, click on the “Verify SMTP Settings” button. You should receive a test email at your account.

Delivery Options (Advanced)

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Email Subject Prefix: This optional string is prefixed to the alert subject. It can be customized to help you identify alerts from specific routers.

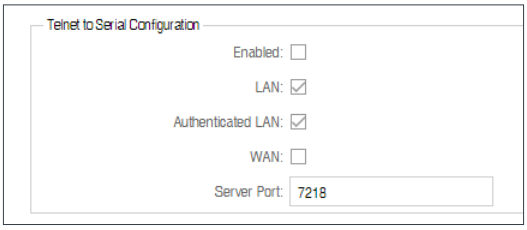
Retry Attempts: The number of attempts made to send an alert to the mail server. After the attempts are exhausted, the alert is discarded.

Retry Delay: The delay between retry attempts.

SERIAL REDIRECTOR

A single USB Serial device can be used to establish a serial link to a host port on the router. The USB Serial device can also be accessed by running "serial" from an SSH session.

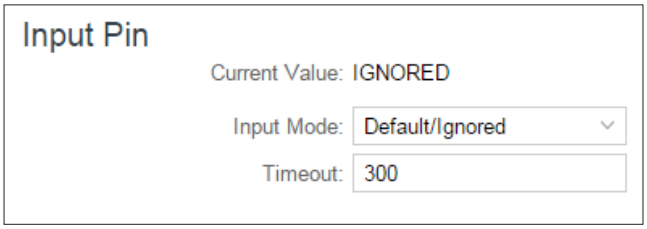
Telnet to Serial Configuration



- **Enabled**: Enabling Telnet to Serial will start a Telnet server that passes its connection to the serial adapter. Enabling this service is not necessary when accessing serial through SSH.
- **LAN**: Enable serial redirector for LAN connections.
- **Authenticated LAN**: Enable serial redirector for Authenticated LAN connections. You must be logged into the router to use the redirector.
- **WAN**: Enable serial redirector for WAN connections.
- **Server Port**: Enter a port number for the redirector to use. (Default: 7218)

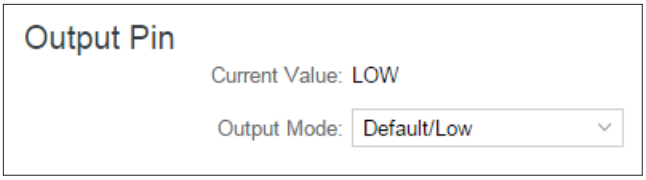
GPIO CONNECTOR

Input Pin



- **Default/Ignored:** In this mode the input pin is not used.
- **Ignition Sensing:** In this mode the router will turn off after the input has been held low for the timeout period in seconds. The router will then reboot when the input is returned to high. If the input is held low for less than the timeout period before returning to high, no action is taken.
- **Input Sensing:** In this mode the logic state (high or low) is automatically sensed by the router and is readable as the Current Value.
- **Router Reset:** In this mode an external device can reset the router by holding the input low for 10-seconds.

Output Pin



- **Default/Low:** In this mode the output pin is not used and is at 0V (ground potential).
- **Set High/Router Running:** In these modes the output pin is logic low while the router is booting and transitions to logic high when the router is fully running. If the router is reset, the output returns to low until the router has fully rebooted.
- **Modem Connected:** In this mode the output pin is logic low until the modem has connected to the tower. If the connection drops, this output is set low until the connection is restored.

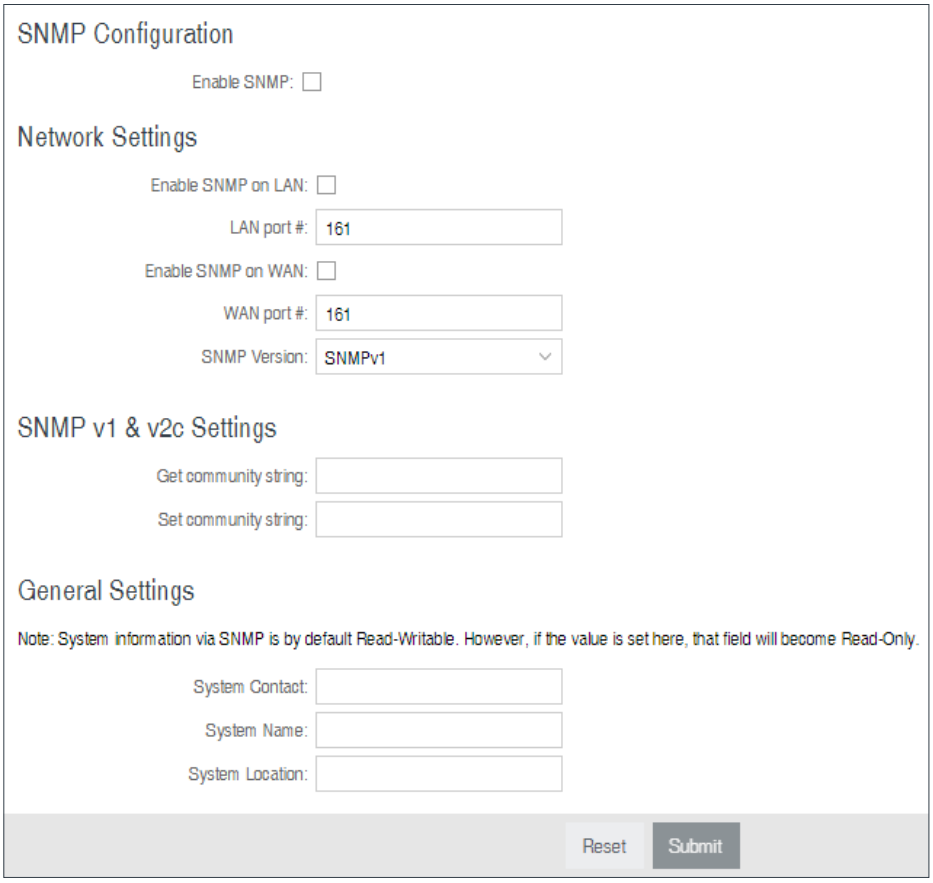
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

SNMP CONFIGURATION

SNMP, or Simple Network Management Protocol, is an Internet standard protocol for remote management. You might use this instead of NetCloud Manager if you want to remotely manage a set of routers that include both Cradlepoint and non-Cradlepoint products.

SNMP Configuration

- **Enable SNMP**: Selecting "Enable SNMP" will reveal the router's SNMP configuration options.



Network Settings

- **Enable SNMP on LAN**: Enabling SNMP on LAN will make SNMP services available on the LAN networks provided by this router. SNMP will not be available on guest or virtual networks that do not have administrative access.
- **LAN port #**: Use the LAN port # field to configure the LAN port number you wish to access SNMP services on. (Default: 161)
- **Enable SNMP on WAN**: Enabling SNMP on WAN will make SNMP services available to the WAN interfaces of the router.
- **WAN port #**: Use the WAN port # field to configure which publicly accessible port you wish to make SNMP services available on. (Default: 161)
- **SNMP Version**
  - **SNMPv1**: SNMP version 1 is the most basic version of SNMP. SNMPv1 will configure the router to transmit with settings compatible with SNMP version 1 protocols.
  - **SNMPv2c**: SNMP version 2c has the same features as v1 with some additional commands. SNMPv2c will configure the router to use settings and data formatting compatible with SNMP version 2c.
  - **SNMPv3**: SNMP version 3 includes all prior features with security available. SNMPv3 is the most secure setting for SNMP. If you wish to configure traps then you must use SNMP version 3.

SNMP v1 & v2c Settings

- **Get community string**: The "Get community string" is used to read SNMP information from the router. This string is like a password that is transmitted in regular text with no protection.
- **Set community string**: The "Set community string" is used when writing SNMP settings to the router. This string is like a password. It is a good idea to make it different than the "Get community string."

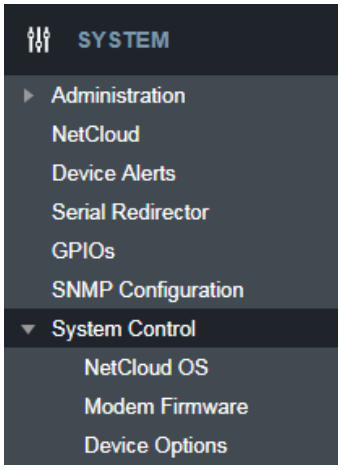
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

SNMPv3
If you select SNMPv3, you have several additional configuration options for added security.

- **Authentication type**: Select the authentication and encryption type that will be used when connecting to the router from the following dropdown list. These settings must match the configuration used on any SNMP clients.
- **MD5 with no encryption**
- **SHA with no encryption**
- **MD5 with DES encryption**
- **SHA with DES encryption**
- **MD5 with AES encryption**
- **SHA with AES encryption**
- **Username**: Enter the Username configured on your SNMP host in the username field.
- **Password**: Enter the Password for your SNMP host in the password and verify password fields. This password must be at least eight characters long.
- **Enable SNMP traps**: Enabling traps will allow you to configure a destination server, community, and port for trap notifications. Trap notifications are returned to the server with SNMPv1.
- **Trap community string**: The trap notifications will be returned to the trap server using this SNMPv1 trap community name.
- **Address for trap server**: Enter the address of the host system that you want trap alerts sent to.
- **Trap server port #**: Enter the port number that the remote host will be listening for trap alerts on. (Default: 162)

General Settings
System information via SNMP is Read-Writable by default. However, if a value is set here, that field will become Read Only.

- **System Contact**: Input the email address of the system administrator.
- **System Name**: Input the router's hostname.
- **System Location**: Input the physical location of the router. This is simply a string for your own information.



SYSTEM CONTROL

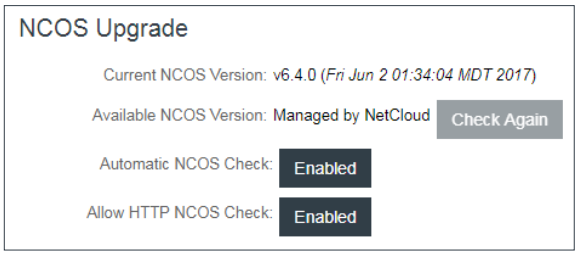
NETCLOUD OS

This allows the administrator to load new NetCloud OS onto the router to add new features or fix defects. If you are happy with the operation of the router, you may not want to upgrade just because a new version is available. Check the NCOS release notes for information to decide if you should upgrade.

Current NCOS Version: Shows the number of the current NCOS and the date it was updated.

Available NCOS Version: If there is a new NCOS version available, this will list the version number. Click "**Check Again**" to have the router check for the newest NCOS.

Automatic NCOS Check: Automatically check for new NCOS updates once daily.

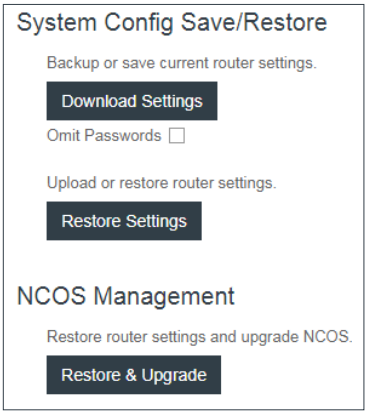

NCOS Upgrade
Current NCOS Version: v6.4.0 (Fri Jun 2 01:34:04 MDT 2017)
Available NCOS Version: Managed by NetCloud
Check Again
Automatic NCOS Check: Enabled
Allow HTTP NCOS Check: Enabled

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Manual NCOS Upload: Upload the router OS from an attached computer. (Go to **cradlepoint.com/firmware** to download the router OS.)

System Config Save/Restore
Download Settings: Click on "**Dowload Settings**" to save your current settings to a file on a computer.
Restore Settings: Click on "**Restore Settings**" to restore your previous settings from a file on a computer.

NCOS Management
Load new NCOS and restore your previous settings from a file on a computer without rebooting between steps.

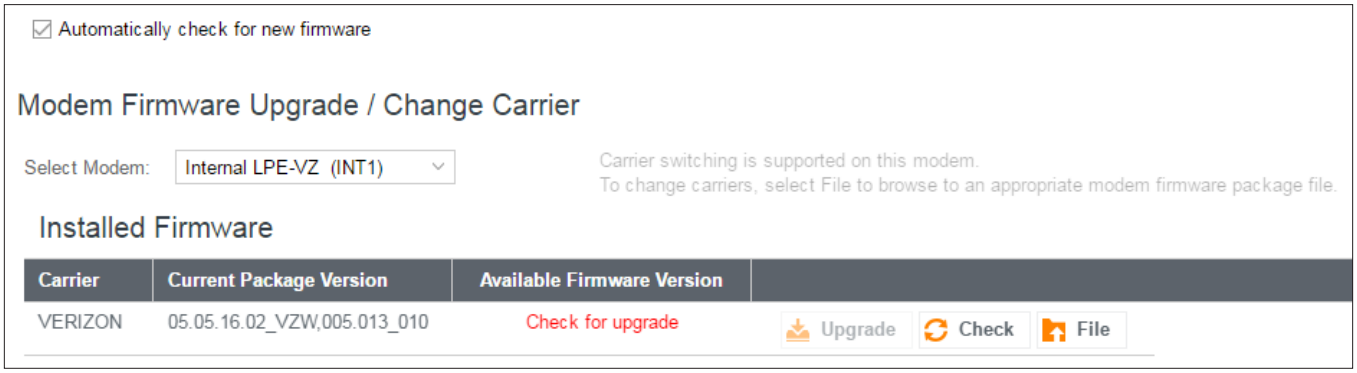


MODEM FIRMWARE

This allows the administrator to load new firmware onto Cradlepoint modems attached to the router. Note that modem firmware is separate from router OS. New modem firmware may be necessary to update the module due to carrier updates or defect resolution. If you are happy with the operation of the modem, you may not want to upgrade just because a new version is available. Please check the modem firmware release notes for information to decide if you should upgrade or not.

Most Cradlepoint modems contain a single firmware image that can be Checked, Updated or manually updated. With some modems (such as LPE), you have the ability to change the firmware to support a different carrier image. With other select modems (such as LP6), more than one modem firmware image may be locally stored within the device's memory.

You must first select the Cradlepoint modem you would like to update. Once selected, the appropriate modem firmware update options will display.



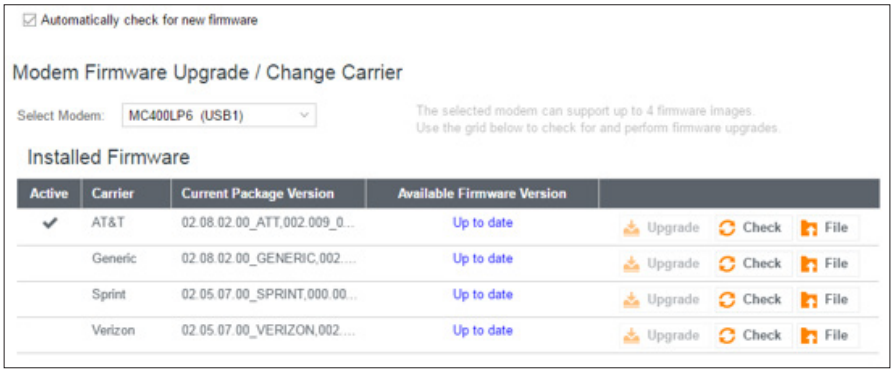
For modems supporting manual carrier switching (such as LPE), select **File** to browse to an appropriate, different modem firmware package file to load into the modem's memory.

Firmware updates can be performed on any firmware line item using the **Check/Upgrade** or **File** (manual) process.

The following actions are available to be configured:

- **Automatically check for new firmware:** Click the checkbox to indicate whether the system is to automatically check for available modem firmware updates. When enabled, the system checks once a day. This global setting applies to all modems connected to the router.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com



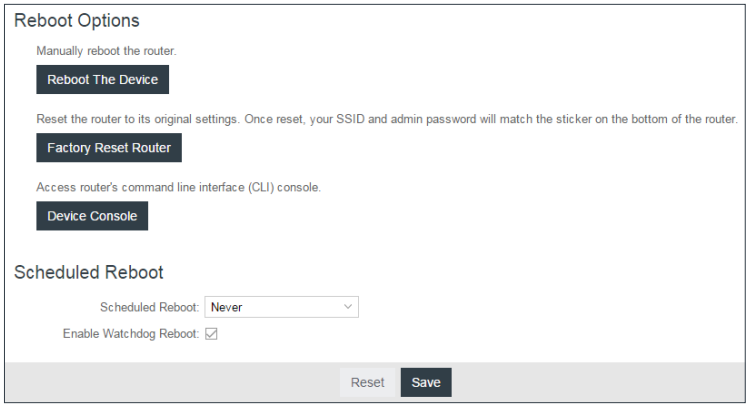
- **Select Modem**: Select the appropriate modem which you would like to update. Note that dual SIM devices are listed as a single modem.

In the Installed Firmware grid, you will see the following columns:

- **Active (Multi-firmware modems only)**: Indicates which carrier package is currently active on the modem. *Note: You cannot select the active image. On multi-firmware modems, the carrier firmware is selected automatically.*
- **Carrier**: Displays the carrier supported by the modem firmware. For carriers not otherwise available, "Generic" will be displayed.

DEVICE OPTIONS

Reboot Options


Reboot Options
Manually reboot the router.
Reboot The Device
Reset the router to its original settings. Once reset, your SSID and admin password will match the sticker on the bottom of the router.
Factory Reset Router
Access router's command line interface (CLI) console.
Device Console
Scheduled Reboot
Scheduled Reboot: Never
Enable Watchdog Reboot:
Reset
Save

- **Reboot the Device**: Manually restart the router.
- **Factory Reset Router**: Reset the router to its original settings. Once reset your SSID and admin password will match the sticker on the bottom of the router.
- **Device Console**: Access router's command line interface (CLI) console.

Scheduled Reboot

- **Scheduled Reboot**: Router will restart at user-specified time.
- **Enable Watchdog Reboot**: Router will restart when it determines an unrecoverable error condition has occurred.

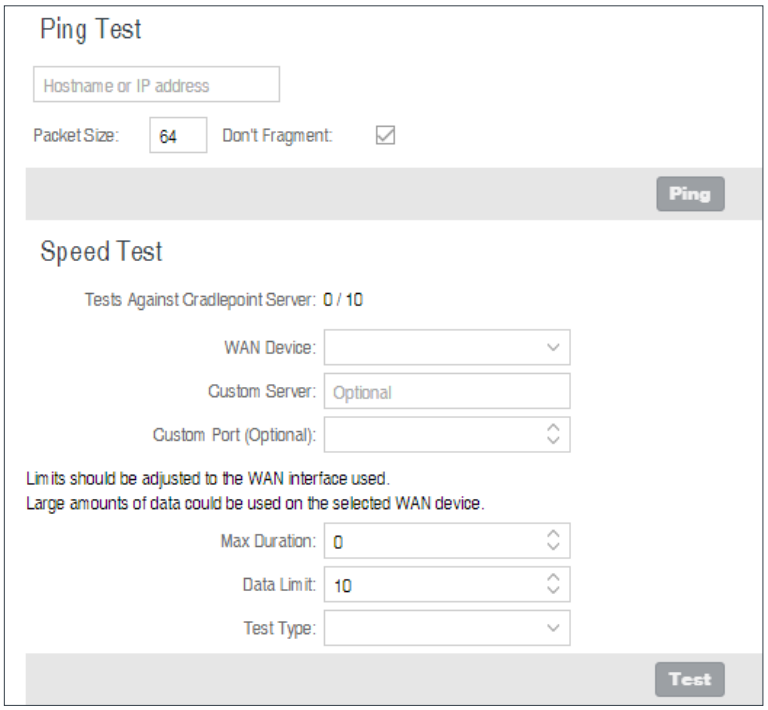
DIAGNOSTICS

Ping Test

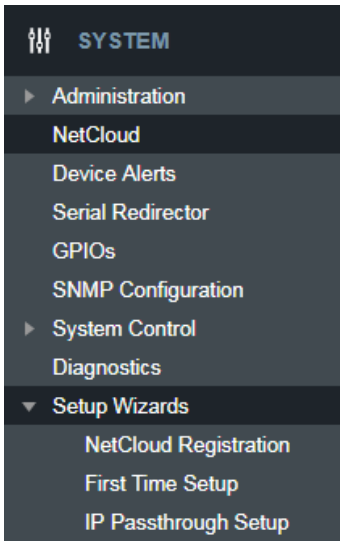
A simple test to check Internet connectivity. Type the Hostname or IP address of the computer you want to ping and click the '**Ping**' button.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

Speed Test



- **Tests Against Cradlepoint Server** - Up to ten speed tests are permitted against a Cradlepoint server.
- **WAN Device** - The WAN Device that is selected will have the test run on it. If no device is selected then the highest priority connected device will be used.
- **Custom Server** - Type the Hostname or IP address of the server to which you wish to perform a test. If left empty the test will be done to a Cradlepoint server.
- **Custom Port (Optional)** - The port to which the test is directed.
- **Max Duration** - The Max Duration is the Maximum amount of time for which the test should be run. The test may finish sooner if sufficient data is collected.
- **Data Limit** - The Data Limit is the limit of how much data will be transferred while measuring the connection speed; this should be limited to reduce the expense of a speed test. Setting the limit to 0 will cause the test to run until enough data is collected or the duration limit is met.
- **Test Type** - Select the type of test you would like to run. TCP Upload will test speed going to the server, TCP Download will test speed coming to the client, and UDP will measure the speed going to the server.



SETUP WIZARDS

NETCLOUD REGISTRATION

To register the router with Cradlepoint NCM you must first have an account. If you need to create an account you can signup at **cradlepoint.com**.

Once you've created an account, or if you already have one, you can enter your NCM username and password to register the router.

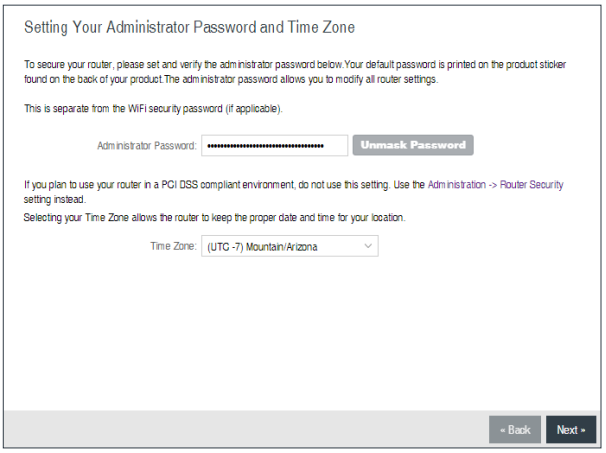
©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

FIRST TIME SETUP

Administrator Password and Time Zone

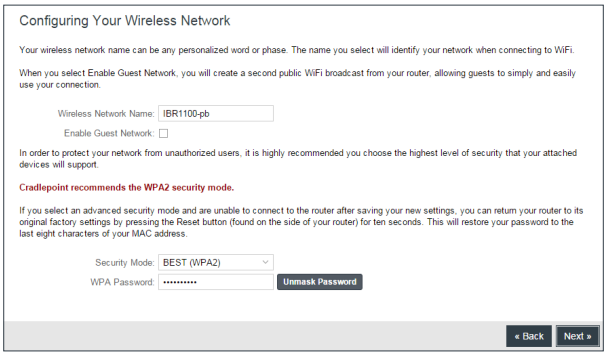
Enter a password for the administrator who will have full access to the router's management interface.

You can use the default password on the back of your product, or you can create a custom Administrator Password.


Setting Your Administrator Password and Time Zone
To secure your router, please set and verify the administrator password below.Your default password is printed on the product sticker found on the back of your product.The administrator password allows you to modify all router settings.
This is separate from the WiFi security password (if applicable).
Administrator Password:
Unmask Password
If you plan to use your router in a PCI DSS compliant environment, do not use this setting. Use the Administration -> Router Security setting instead.
Selecting your Time Zone allows the router to keep the proper date and time for your location.
Time Zone:
(UTC -7) Mountain/Arizona
« Back
Next »

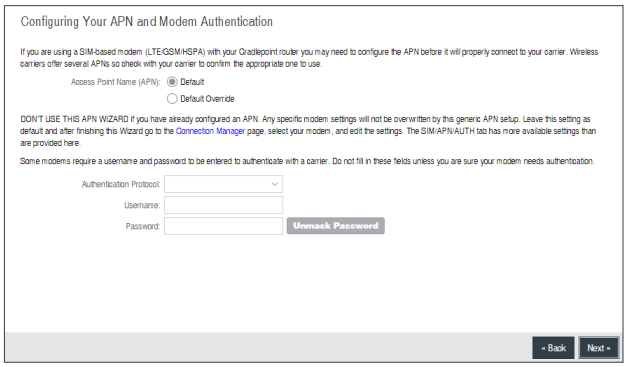
Configuring Your Wireless Network

- **Wireless Network Name** - When you are browsing for available wireless networks, this is the name that will be broadcast from this router. This name is also referred to as the SSID. For security purposes, it is highly recommended you change the pre-configured wireless network name.
- **Enable Guest Network** - If the guest network is enabled, anyone can connect to the special guest network which allows limited connectivity to the Internet while preventing access to your local network.
- **Security Mode**
  - **Best (WPA2)**: Select this option if your wireless adapters support WPA2-only mode. This will connect to most new devices and is the most secure, but may not connect to older devices or some handheld devices such as a PSP.
  - **Good (WPA1 & WPA2)**: Select this option if your wireless adapters support WPA or WPA2. This is the most compatible with modern devices and PCs.
  - **Poor (WEP)**: Select this option if your wireless adapters only support WEP. This should only be used if a legacy device that only supports WEP will be connected to the router. WEP is insecure and obsolete and is only supported in the router for legacy reasons. The router cannot use 802.11n modes if WEP is enabled; router WiFi performance and range will be limited.
  - **None (OPEN)**: Select this option if you do not want to activate any security features.
- **WPA Password** - The WPA Password must be between 8 and 64 characters long. A combination of upper and lower case letters along with numbers and special characters is recommended to prevent hackers from gaining access to your network.


Configuring Your Wireless Network
Your wireless network name can be any personalized word or phase. The name you select will identify your network when connecting to WiFi.
When you select Enable Guest Network, you will create a second public WiFi broadcast from your router, allowing guests to simply and easily use your connection.
Wireless Network Name:
IBR1100-pb
Enable Guest Network:
In order to protect your network from unauthorized users, it is highly recommended you choose the highest level of security that your attached devices will support.
Cradlepoint recommends the WPA2 security mode.
If you select an advanced security mode and are unable to connect to the router after saving your new settings, you can return your router to its original factory settings by pressing the Reset button (found on the side of your router) for ten seconds. This will restore your password to the last eight characters of your MAC address.
Security Mode:
BEST (WPA2)
WPA Password:
Unmask Password
« Back
Next »

Configuring Your APN and Modem Authentication

If you are using a SIM-based modem (LTE/GSM/HSPA) with your Cradlepoint router you may need to configure the APN before it will properly connect to your carrier. Wireless carriers offer several APNs so check with your carrier to confirm the appropriate one to use. You can use the default password on the back of your product, or you can create a custom Administrator Password.


Configuring Your APN and Modem Authentication
If you are using a SIM-based modem (LTE/GSM/HSPA) with your Cradlepoint router you may need to configure the APN before it will properly connect to your carrier. Wireless carriers offer several APNs so check with your carrier to confirm the appropriate one to use.
Access Point Name (APN):
Default
Default Override
DON'T USE THIS APN WIZARD if you have already configured an APN. Any specific modem settings will not be overwritten by this generic APN setup. Leave this setting as default and after finishing this Wizard go to the Connection Manager page, select your modem, and edit the settings. The SIM/APN/AUTH tab has more available settings than are provided here.
Some modems require a username and password to be entered to authenticate with a carrier. Do not fill in these fields unless you are sure your modem needs authentication.
Authentication Protocol:
Username:
Password:
Unmask Password
« Back
Next »

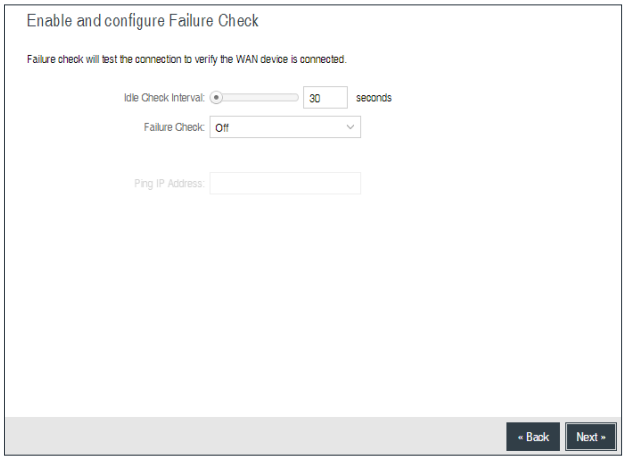
NOTE: *DO NOT USE THIS APN WIZARD* if you have already configured an APN. Any specific modem settings will not be overwritten by this generic APN setup. Leave this setting as default and after finishing this Wizard go to the

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

CONNECTION MANAGER page, select your modem, and edit the settings. The SIM PIN/APN tab has more available settings than are provided here.

Some modems require a username and password to be entered to authenticate with a carrier. Do not fill in the following fields unless you are sure your modem needs authentication.

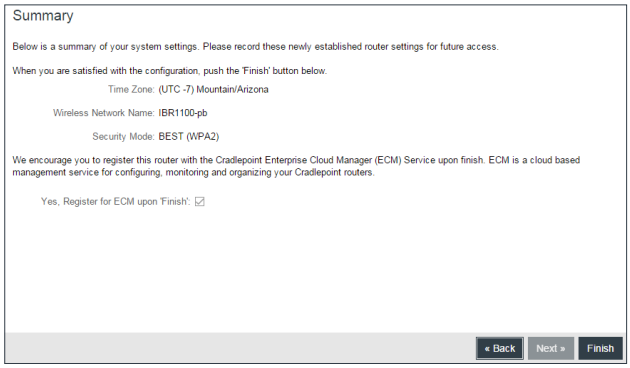
- Authentication Protocol
- Username
- Password



Enable and Configure Failure Check

Failure check will test the connection to verify the WAN device is connected.

- **Idle Check Interval**: Set the number of seconds the router will wait between checks to see if the WAN is still available.
- **Failure Check**:
  - **Off**: Once the link is established the router takes no action to verify that it is still up.
  - **On**: Modems will be set to use the Passive DNS failure check type. Ethernet and WiFi as WAN connections will be set to use Active Ping.
- **Ping IP Address**: This IP address must be an address that can be reached through your WAN connection (modem/Ethernet). Some ISPs/Carriers block certain addresses, so choose an address that all of your WAN connections can use.


Summary
Below is a summary of your system settings. Please record these newly established router settings for future access.
When you are satisfied with the configuration, push the 'Finish' button below.
Time Zone: (UTC -7) Mountain/Arizona
Wireless Network Name: IBR1100-pb
Security Mode: BEST (WPA2)
We encourage you to register this router with the Cradlepoint Enterprise Cloud Manager (ECM) Service upon finish. ECM is a cloud based management service for configuring, monitoring and organizing your Cradlepoint routers.
Yes, Register for ECM upon 'Finish':
« Back
Next »
Finish

Summary

Review your settings and click **Finish** to exit or **Back** to edit.

IP PASSTHROUGH SETUP

IP passthrough takes a 3G/4G WAN data source (USB, ExpressCard, or Cradlepoint business-grade modem) and passes the IP address through to Ethernet LAN.

Enabling IP passthrough will make many changes to your router configuration. Please review this list and ensure they are compatible with how the router will be used.

- All Ethernet ports will be set to LAN
- All network groups except the primary network group will be removed
- All WAN devices will have Load Balance disabled and the highest priority device will be used
- All Wireless interfaces will be removed from the primary network group
- All Router based VPN and GRE services will be disabled
- The Routing Mode will be set to IP Passthrough
- The Subnet Selection Mode will be set to "Automatically Create Subnet" unless overridden via the **Subnet Selection Mode** dropdown

Any Ethernet WAN connections should be disconnected before IP passthrough is enabled.

©2017 Cradlepoint. All Rights Reserved. | +1.855.813.3385 | cradlepoint.com

APPENDIX

OPEN SOURCE SOFTWARE

This product contains software distributed under one or more of the following open source licenses: GNU General Public License Version 2, BSD License, Net-SNMP License, and PSF License Agreement for Python 3.3. For more information on this software, including licensing terms and your rights to access source code, contact Cradlepoint at **cradlepoint.com/opensource**.

WARRANTY INFORMATION

Cradlepoint, Inc. warrants this product against defects in materials and workmanship to the original purchaser for a period of three (3) years from the date of shipment. This warranty is limited to a repair or replacement of the product, at Cradlepoint's discretion, as purchaser's sole and exclusive remedy. Cradlepoint does not warrant that the operation of the device will meet your requirements or be error free.

LIMITATION OF CRADLEPOINT LIABILITY

The information contained in this Safety, Regulatory, and Warranty Guide is subject to change without notice and does not represent any commitment on the part of Cradlepoint or its affiliates. CRADLEPOINT AND ITS AFFILIATES HEREBY SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL: (A) DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION FOR LOSS OF PROFITS OR REVENUE OR OF ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE THE DEVICE, EVEN IF CRADLEPOINT AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF SUCH DAMAGES ARE FORESEEABLE; OR (B) CLAIMS BY ANY THIRD PARTY. NOTWITHSTANDING THE FOREGOING, IN NO EVENT SHALL THE AGGREGATE LIABILITY OF CRADLEPOINT AND/OR ITS AFFILIATES ARISING UNDER OR IN CONNECTION WITH THE DEVICE, REGARDLESS OF THE NUMBER OF EVENTS, OCCURRENCES, OR CLAIMS GIVING RISE TO LIABILITY, EXCEED THE PRICE PAID BY THE ORIGINAL PURCHASER OF THE DEVICE.

PRIVACY

Cradlepoint collects general data pertaining to the use of Cradlepoint products via the Internet including, by way of example, IP address, device ID, operating system, browser type and version number, etc. To review Cradlepoint's privacy policy, please visit **cradlepoint.com/privacy**.

OTHER BINDING DOCUMENTS; TRADEMARKS; COPYRIGHT

By activating or using your IBR600 or IBR650 device, you agree to be bound by Cradlepoint's Terms of Use, User License and other applicable Legal Policies.

© 2017 Cradlepoint, Inc. All rights reserved. Cradlepoint is not responsible for omissions or errors in typography or photography. Cradlepoint, IBR600, IBR650, and the Cradlepoint logo are trademarks of Cradlepoint, Inc. in the US and other countries. Other trademarks are property of their respective owners.

ROUTER COMMUNICATION/DATA USAGE

The factory default configuration of the router is set to communicate with Cradlepoint and other resources at regular intervals to access the latest NCOS and modem updates, clock synchronization (NTP), and NetCloud Manager (NCM) membership. Such communication may result in data usage and applicable charges regardless of whether the router uses a wired or wireless Internet connection. To avoid such data usage and potential charges, consult the following Knowledge Base article:

http://knowledgebase.cradlepoint.com/articles/support/router-communication-data-usage